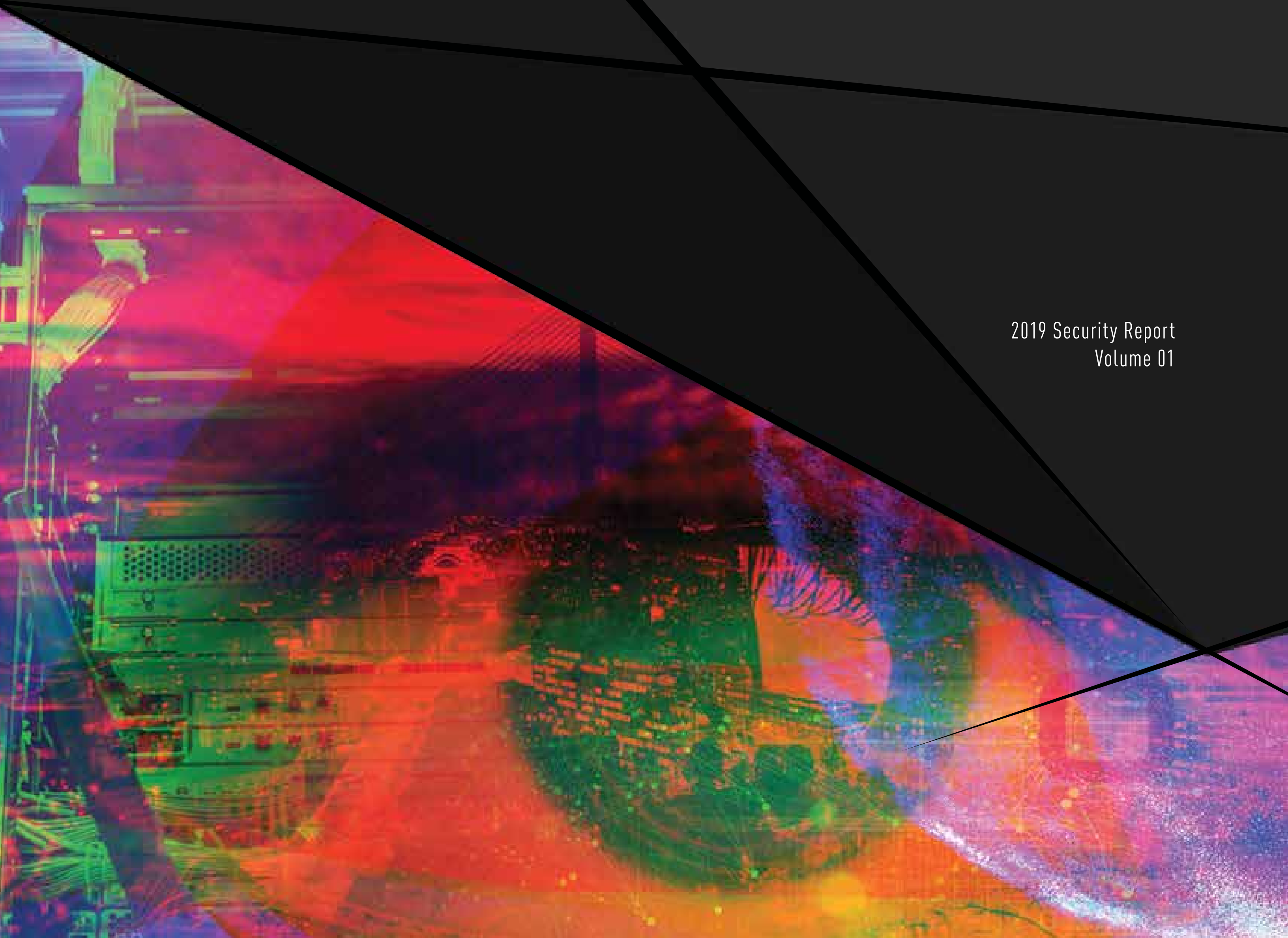
CHECK POINT RESEARCH

CYBER ATTACK TRENDS ANALYSIS

KEY INSIGHTS TO GEAR UP FOR IN 2019

2019 Security Report
Volume 01



VOLUME 01

2019 SECURITY REPORT

INTRODUCTION: METHODOLOGY

2018 introduced a challenging threat landscape. Threat actors consistently improved their cyber weapons and quickly adopted new methods and adapted their attacks to emerging technologies. And although it may have seemed the past year was quieter, this is far from the case.

While threat actors were trying hard to keep a lower profile with their menacing activities, they could not escape our watchful eye. Indeed, never does a day go by that we do not see organizations under constant attack from the ever growing number of malware spreading at higher rates than ever.

In this first installment of the 2019 Security Report we review the latest threats facing organizations in the fifth generation of the cyber landscape and provide you with our observations and insights from the past year. From massive data breaches and crippling ransomware attacks to a meteoric rise in cryptojackers, there was no shortage in disruption caused to global organizations.

With data drawn from our ThreatCloud World Cyber Threat Map and our experience within the cyber research community, we will give a comprehensive overview of the trends observed in the categories of Cryptominers, Ransomware, Malware techniques, Data Breaches, Mobile and Nation State cyber attacks.

We will then conclude with a review of the predictions made in our 2018 Security Report and assess to what extent these proved accurate. Along the way we will also provide cutting edge analysis from our in-house experts to arrive at a better understanding of today's threat landscape.

Having mapped out today's current threat landscape, we will then be in a good position in the second installment of this Security Report to take a closer look under the hood of today's cybercrime world and show how this ecosystem remains a key component of the cyber threat landscape.

OVERVIEW: MAJOR CYBER ATTACKS

JAN

$534 million is stolen from Japan's largest digital currency exchange.

Coincheck

FEB

AdultSwine, a mobile malware infecting children's game apps with adware, is downloaded by up to 7 million users.

MAR

The City of Atlanta suffers an attack that locks down city systems for over a week.

APR

Saks Fifth Avenue

Saks 5th Avenue and Lord & Taylor have five million customers' credit card details stolen.

MAY

Users of Copenhagen's city bikes are denied access due to the system being hacked.

JUN

EXACTIS

340 million records of Americans and business are leaked from the Florida-based marketing firm.

JUL

Singapore suffers its biggest cyber attack with the theft of 1.5 million patient records, including the Prime Minister's.

SingHealth

AUG

BRITISH AIRWAYS

Hackers attack British Airways' mobile app and steal credit card details of almost 400,000 customers.

SEP

30 million Facebook users' phone numbers and personal details are exposed in a major breach of privacy.

facebook

OCT

ONWASA

Onslow Water and Sewer Authority suffers a ransomware attack impeding efforts to provide services.

NOV

Hackers steal the personal details of 500 million Marriot owned Starwood Hotel customers.

Marriott
HOTELS · RESORTS · SUITES

DEC

THE WALL STREET JOURNAL.

Ransomware causes printing and delivery disruptions to the LA Times, WSJ and NYT newspapers.

2018: THREAT TRENDS

RANSOMWARE

Atlanta Ransomware Attack

In March, the SamSam ransomware struck the City of Atlanta in a big way by infecting and halting the operation of multiple city services for over a week. Services affected were the city's law courts that prevented court cases from proceeding, warrants being issued, and residents able to access the city fine online payment services. The malware entered through one of the many public-facing entry points, such as FTP servers and various VPNs, and demanded a ransom of almost $7,000 be paid in Bitcoin to unlock each affected computer.

Ukraine Energy Ministry

In April, threat actors used ransomware to take the website of Ukraine's energy ministry offline and encrypt its files. It's believed that threat actors took advantage of vulnerabilities in Drupal 7, the off-the-shelf content management system software, to carry out the attack. Check Point Research carried out a detailed analysis of the vulnerabilities in versions 6-8 of Drupal to reveal how it works.

> ***$2.7 million*** *spent by the City of Atlanta to repair damage from ransomware attack.*
>
> Source: Atlanta Journal-Constitution newspaper – www.ajc.com

Boeing Ransomware Attack

WannaCry ransomware attacks were still active in 2018, as seen in the attack on a Boeing production plant in Charleston, South Carolina. The attack was spread rapidly throughout the company's manufacturing IT systems and there was concern that the virus would hit equipment used in functional tests of planes and potentially spread to airplane software.

Ransomware took center stage in 2017, though last year saw a dramatic fall in this type of attack. Regardless of the decline, however, ransomware attacks have not disappeared, and instead continue to be a major cause of concern for organizations across all industries worldwide.

According to our research into the GandCrab ransomware, threat actors are merely adapting their techniques, sometimes in real time, offering an affiliate system to allow technically low-level criminals to get in on the lucrative form of attack.

Itai Greenberg
VP of Product Management

DATA BREACHES

Facebook Data Breach

In March, reports emerged of how Cambridge Analytica, a political data firm, collected the personal data of over 50 million Facebook users via a 'personality test' app that scraped details about people's personalities, social networks, and their engagement on the social platform. The scandal had a major impact on the internet giant and arguably led to a dramatic drop in their share price.

> ***76%*** *of organizations experienced a phishing attack in the past year.*
>
> Source: 2018 IT Professionals Security Report Survey

Exactis Data Breach

In June, Exactis, a marketing and data aggregation firm based in Florida, left a database exposed on a publicly accessible server. The database contained two terabytes of information that included the personal details, including email addresses, physical addresses, phone numbers, and a host of other personal information, of almost 340 million American citizens and businesses.

Marriott Hotels Data Breach

A massive data breach exposed the records of over 500 million customers of the Marriott-owned Starwood Hotels, taking the title of being the world's second largest data breach. Most of those affected had their name, postal address, phone number, email address, passport number and arrival and departure information exposed. Under the GDPR rules, Starwood may face significant financial penalties of up to four percent of its global annual revenue if found to be in breach.

Although data breaches have been occurring continuously, 2018 was a turning point in respect to how data is perceived and how important it is to protect it. With the introduction of GDPR in May, organizations worldwide need to make data protection a priority and be compliant with on a legal and regulatory level.

With cloud becoming an increasingly popular way to store data, either through SaaS services or cloud storage containers, it's become apparent that relying on cloud providers is not enough. Instead, organizations must adopt the Mutual Responsibility model to protect both their data and any means used to access it.

Zohar Alon
Head of Cloud Products

MOBILE MALWARE

'AdultSwine' Malicious Apps

Check Point researchers revealed a new and nasty malicious code on Google Play Store that hides itself inside approximately 60 game apps, several of which are intended for use by children. According to Google Play's data, the apps were downloaded between three million and seven million times. Dubbed 'AdultSwine,' the malicious apps wreaked havoc by displaying ads from the web that are often highly inappropriate and pornographic, attempting to trick users into installing fake 'security apps' and inducing users to register to premium services at the user's expense.

Man in the Disk

A shortcoming in the way Android apps use storage resources was discovered that could open the door to an attack resulting in any number of undesirable outcomes, such as silent installation of unrequested, potentially malicious, apps to the user's phone. The hugely popular game, Fortnite, was found to be susceptible to such an attack and quickly patched a release for its users to install.

> *The 'AdultSwine' malware was installed up to **7 million times** across 60 Children's Games Apps.*
>
> Source: Check Point Research Blog

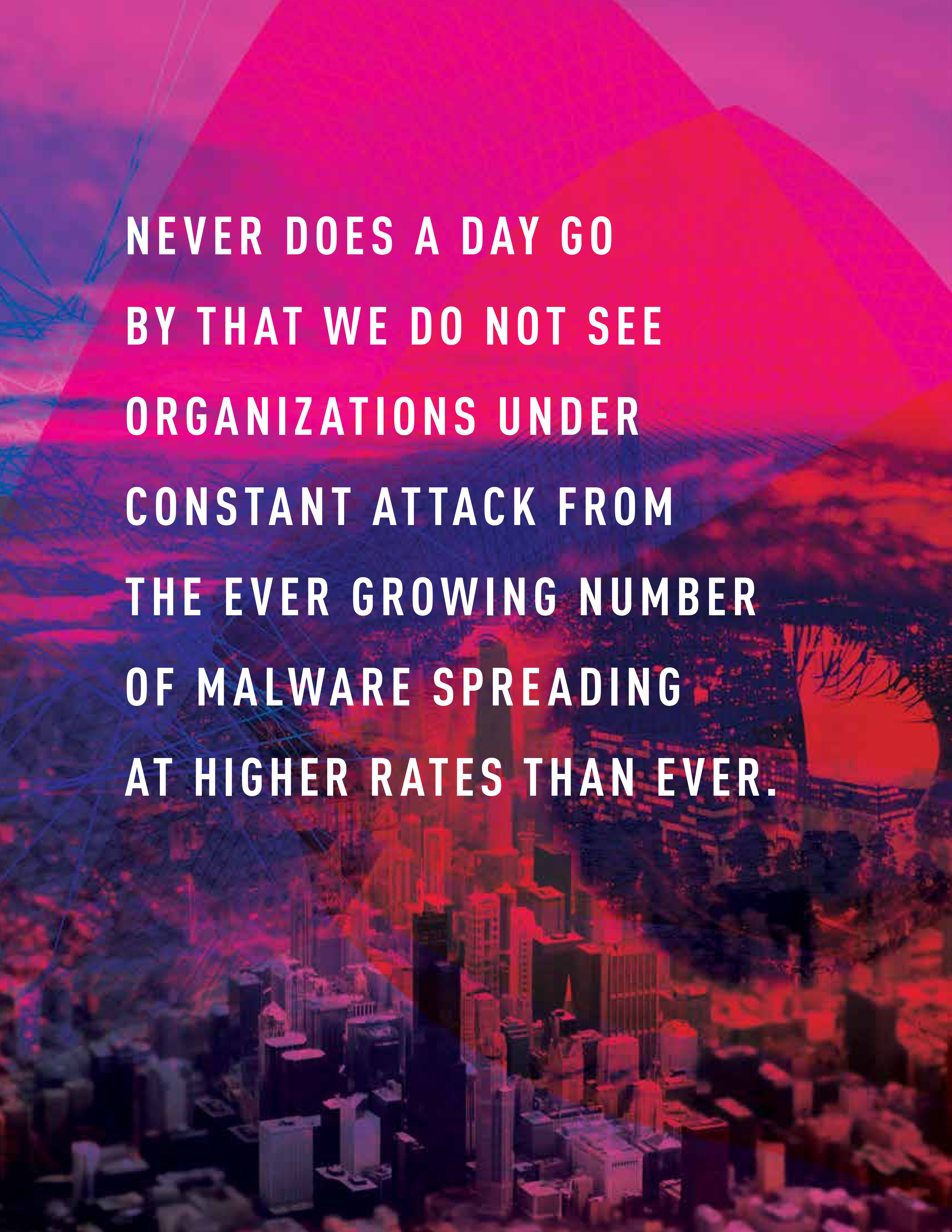
LG Vulnerabilities

Check Point Research discovered two vulnerabilities that reside in the default keyboard on all mainstream LG smartphone models. These vulnerabilities are unique to LG devices, which account for over 20% of the Android OEM market in the US, according to a 2017 survey. Both vulnerabilities could have been used to remotely execute code with elevated privileges on LG mobile devices by manipulating the keyboard updating process, acting as a keylogger and thereby compromising the users' privacy and authentication details. Both vulnerabilities were reported to LG, who then released a patch.

With the mobile threat landscape always evolving, even the most trusted mobile app stores continue to prove themselves insufficient for defending against attacks. Although these stores are improving their own threat prevention technologies, there is still a continuous high infection rate among the world's five billion mobile phone users. This proves why consumers and employees who use their own devices for business activities require their own on-device threat prevention technology as well. The attacks seen over the past year confirms just how vulnerable the data stored on our mobile devices really is.

Brian Gleeson

Head of Threat Prevention
Product Marketing



NEVER DOES A DAY GO BY THAT WE DO NOT SEE ORGANIZATIONS UNDER CONSTANT ATTACK FROM THE EVER GROWING NUMBER OF MALWARE SPREADING AT HIGHER RATES THAN EVER.

CRYPTOCURRENCY ATTACKS

Jenkins Miner

Check Point Research discovered one of the biggest malicious mining operations ever seen. Dubbed 'Jenkins Miner', the operation targeted powerful Jenkins servers using a hybridization of a Remote Access Trojan (RAT) and XMRig miner. Distributed over several months, the cryptomining malware targeted victims around the globe to mine valuable cryptocurrency, negatively impacting organizations' servers by causing slower load times and raising the potential for a Denial of Service.

> ***Over 20%*** *of organizations are impacted by Cryptojacking Malware every week.*
>
> Source: Check Point ThreatCloud

RubyMiner

By using old vulnerabilities published and patched in 2012 and 2013, a threat actor attempted to exploit 30% of all networks worldwide and plant the RubyMiner crytomining malware on their servers to mine the Monero cryptocurrency. Among the top countries targeted were the United States, Germany, United Kingdom, Norway and Sweden, though no country went unscathed.

Coinrail Hacked

The South Korean cryptocurrency exchange, Coinrail, was hacked in June causing the price of Bitcoin to drop sharply by 10%. The hack caused the loss of around 30% of the coins traded (around $35 million worth) on the exchange and highlighted the lack of security and weak regulation of the global cryptocurrency markets. This was the latest in a spate of attacks on virtual coin exchanges; others included Japan's CoinCheck where over $500 million in coin value was stolen.

> ***40%*** *of organizations were impacted by Cryptominers last year.*
>
> Source: Check Point ThreatCloud

The end of 2017 marked the rise of cryptominers, continuing in full force throughout 2018. Unlike ransomware, cryptomining offers cyber criminals a much stealthier style of attack that can remain on an organization's servers for months without being detected. During this time, and as long as it is undetected, its authors earn a steady stream of passive income.

Also in contrast to ransomware, cyber criminals are at much less risk while illicitly making money. Whether it is using a user's private computer, infecting a website with a crypto-mining advertisement or harnessing the immense CPU power of an organization's server, it does not take long for criminals to earn large amounts of their preferred digital currency.

Maya Horowitz
Director of Threat Intelligence & Research

BOTNETS

IoTroop's First Attack

In late January 2018, the 'IoTroop' botnet, discovered by Check Point researchers in October 2017, launched its first attack against the financial sector. IoTroop is a powerful internet of things (IoT) botnet comprised primarily of compromised home routers, TVs, DVRs, and IP cameras. The first attack used 13,000 IoT devices across 139 countries to target a financial organization with a DDoS attack, followed by two more attacks against similar targets within 48 hours.

> *The Ramnit Botnet infected* ***100,000*** *in just two months.*
>
> Source: Check Point Research, Ramnit's Network of Proxy Servers

Pyeongchang Winter Olympics

According to the International Olympic Committee (IOC), a DDoS attack on the Pyeongchang Winter Olympic Games took the official Olympic website offline for 12 hours and disrupted WiFi and televisions at the Olympic stadium. Although critical operations were not affected by the incident, event organizers had to shut down servers and the official games website to prevent further damage.

> ***49%*** *of organizations experienced a DDoS attack in the past year.*
>
> Source: 2018 IT Professionals Security Report Survey

Attack on US Democratic Candidates

In July 2018, hackers targeted the campaigns of at least two US Democrat candidates during the 2018 primary's season. Using DDoS attacks to disrupt campaign websites for over 21 hours, potential voters were denied access to key information or resources during periods of active fundraising and positive news publicity.

Anti-virus software makes recruiting an army of bots to launch a DDoS attack from unprotected computers a tricky task for threat actors. However, with organizations increasingly turning to popular, yet unprotected and vulnerable IoT devices to keep tabs on their operations, the number of opportunities for a large botnet recruitment drive also increases.

It should come as no surprise that, as a result of such large botnet recruitment, we are seeing larger DDoS attacks.

Richard Clayton
Head of Botnet Research

APT ATTACKS

Big Bang APT

The Check Point Threat Intelligence Team discovered the comeback of an APT surveillance attack against institutions across the Middle East, specifically the Palestinian Authority. The attack began with the targets receiving an attachment, sent in a phishing email, which included a malicious executable. The malware's functions included taking a screenshot of the infected machine, logging details about the victim's system and stealing a list of documents with certain file extensions.

> *The US and UK formally blamed Russia for the 2017 NotPetya ransomware attack that caused* ***billions of dollars*** *in damages worldwide.*
>
> Source: Check Point ThreatCloud

SiliVaccine

In exclusive research, Check Point Researchers revealed some alarming details about North Korea's home-grown anti-virus software, SiliVaccine. One of several interesting factors was that a key component of SiliVaccine's code is a direct copy of Trend Micro's anti-virus scanning engine. Known to be sent to foreign journalists that report on North Korean activities, the researchers discovered that SiliVaccine includes highly suspicious behavior that would allow the monitoring of these journalists' activities.

Russia UK Relations

As tensions in UK and Russia relations intensified over UK accusations that Russia poisoned two UK citizens on home soil, the UK's National Cyber Security Centre warned that Russian state actors were targeting UK critical infrastructure by infiltrating supply chains. Although attribution is notoriously difficult, the attacker's techniques seemed to bear the hallmarks of 'Energetic Bear,' a Russian hacking group that has been tied to attacks on the energy sector since 2012.

> ***614 GB of data*** *related to weapons, sensor and communication systems stolen from US Navy contractor, allegedly by Chinese government hackers.*
>
> Source: Check Point ThreatCloud

Over the past year, a rare glimpse into APT attacks has shown that nation state and non-state organizations will go to great lengths in order to gain intelligence on their adversaries.

Government agencies must be on high alert for the clear and present threat of cyber warfare. It's an act of aggression that remains and will continue to be an attractive weapon of choice due to its high impact, low risk of attribution and cost effectiveness.

Dan Wiley

Head of Incident Response

2018 TRENDS ANALYSIS

Cryptomining Is Here to Stay

At the beginning of 2018, cryptomining malware made a magnificent rise utilizing a wide-scope of targets including personal computers,[1] powerful servers,[2] mobile devices,[3] and even the cloud environment.[4] When it comes to mining there is no doubt that they are here to stay. Indeed, cryptomining attacks soared in 2018, affecting over 40% of organizations worldwide at its peak, compared to 20.5% at the end of 2017, and dominated the top cyber-attacks[5] and malware families seen in the wild for 12 months straight.

In January 2018, total cryptocurrency values dropped rapidly, shrinking[6] by about 86% from their peak. Despite this, cryptominers detached themselves from cryptocurrencies' market cap and kept their place as the most prominent malware infection used by threat actors in 2018.

As we will see in the next installment of this Security Report, from an attackers' perspective, cryptojackers can be highly lucrative, are simple to launch and easy to conceal. Furthermore, cryptojacking attacks allow threat actors to carefully walk the thin line of legitimacy, knowing that cryptojacking is not considered as offensive as other attack techniques such as ransom extortion or data theft.

In the second half of 2018, due to the attention they gained from security vendors, cryptojackers went through a rapid evolution, becoming more sophisticated and capable of overcoming security solutions. As a result, we witnessed cryptojackers that presented various evasion techniques[7], quick adoption of exploits, and even those embedded in multi-staged attacks to serve additional malware[8] to the infected machine.

When it comes to mining it seems threat actors have become more creative and continue to invent increasingly deceptive techniques to serve miners. These include drive-by attack kits and implanting miners inside legitimate applications' installers such as Flash update and Windows Installer.

A year after they took the world by storm, cryptominers show no intention of slowing down soon. New, sophisticated malware families keep integrating mining capabilities to their code and tens of thousands of websites are constantly compromised to exploit their users' resources.

---

[1] https://www.bleepingcomputer.com/news/security/winstarnssmminer-coinminer-campaign-makes-500-000-victims-in-three-days/

[2] https://research.checkpoint.com/jenkins-miner-one-biggest-mining-operations-ever-discovered/

[3] https://securityaffairs.co/wordpress/70968/malware/hiddenminer-android-miner.html

[4] https://motherboard.vice.com/en_us/article/8x5wy5/cryptocurrency-tesla-bitcoin-mine-ethereum

[5] http://blog.checkpoint.com/2018/12/11/november-2018s-most-wanted-malware-the-rise-of-the-thanksgiving-day-botnet/

[6] https://coinmarketcap.com/charts/

[7] https://www.kaspersky.com/about/press-releases/2018_new-fileless-crypto-miner

[8] https://securityaffairs.co/wordpress/75070/malware/zombieboy-monero-miner.html

Ransomware Attacks Go Boutique

Ransomware is today a household term even among non-technical-oriented individuals. In the last four years it has spread massively, in large-scale campaigns, targeting all industries and successfully sowing panic in their victims, prompting them to pay any sum in ransom to retrieve their data safely.

In 2018, however, we witnessed Ransomware adapting to become more targeted to ensure more lucrative profits. This evolution is a direct result of a noted decrease in the actual ransom payments, probably derived from the growing security awareness and mitigation techniques adopted by many companies, including routine back-up policies and the free availability of decryption tools.

This new strategy allows threat actors to maximize their revenue, as a tailored attack against organizations' critical assets is a great tactic to ensure the ransom payments. Furthermore, it allows cybercrime to enter safely under the radar of security vendors, by not engaging with a mass distribution campaign which is likely to lead to more exposure.

This year the SamSam Ransomware reaped millions in cryptocurrencies after shutting down Atlanta[9] and Colorado[10] city councils' departments, hospitals,[11] and the medical testing giant LabCorp.[12] In other cases the port of Barcelona and the port of San Diego suffered major Ransomware attacks that significantly disrupted critical operations. Another strain of Ransomware also hit Bristol Airport[13] in the UK, and shut down flight display screens for two days.

As victims of targeted Ransomware attacks don't usually disclose the full damage and attack details, these cases are probably only a drop in the ocean of the actual total attacks launched using this strategy. The equation is simple though; the greater the potential damage, the higher the chance the ransom will be paid.

In addition, the infection stage, previously dominated by vast spam or drive-by methods, was replaced by an extensive reconnaissance effort aimed to locate the most lucrative targets. This involves searching unsecured Remote Desktop Protocol (RDP) connections, manual network mapping and credential purchasing in hacking forums. The Ryuk Ransomware,[14] for example, exposed by Check Point security researchers in August 2018, had conducted highly-planned and sophisticated attacks against well-chosen organizations and netted $640,000 for its operators. While working on this report, Ryuk hit the newspaper print and online media publishing company, Tribune Publishing,[15] and prevented the distribution of many leading U.S. newspapers, including the Wall Street Journal, New York Times and Los Angeles Times.

---

[9] https://www.bleepingcomputer.com/news/security/city-of-atlanta-it-systems-hit-by-samsam-ransomware/

[10] http://securityaffairs.co/wordpress/69492/malware/samsam-ransomware-colorado-dot.html

[11] http://securityaffairs.co/wordpress/68052/malware/samsam-ransomware-campaign.html

[12] https://www.csoonline.com/article/3291617/security/samsam-infected-thousands-of-labcorp-systems-via-brute-force-rdp.html

[13] https://securityaffairs.co/wordpress/76248/breaking-news/bristol-airport-cyber-attack.html

[14] https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/

[15] https://www.forbes.com/sites/daveywinder/2018/12/30/north-korea-implicated-in-attack-that-stops-wall-street-journal-and-new-york-times-presses/#63ca369220a2

Malware Synergy

The shift of prominent malware families, such as the Emotet[16] Banking Trojan, from banking credential theft to the distribution business, marks a significant phenomenon observed in 2018. Malware families previous known for their single, well-functioning utility are now expanding their operations and offering additional capabilities. Furthermore, new malware families are often released to the wild with more than one significant goal or attack vector.

Hybrid malware, which demonstrate a few and often entirely different functions, are a great way for an attacker to guarantee that their operation yields profits. One example, a ransom demand that is deployed together with collecting user credentials, or harvesting sensitive information for future phishing attack. Another example, a botnet that can perform cryptocurrency mining using the bot network's CPU resources, and in parallel, utilize the same bots to distribute email spam.

These functions, though, do not have to be carried out by the same malware. Often, two malware developers could join forces in a single campaign involving different malware strains, either to ensure revenues and success or to achieve multiple goals.

In October 2018, computers and servers of North Carolina's Onslow Water and Sewer authority were attacked by the Ryuk ransomware, a highly-targeted, manually operated family. Interestingly, the investigation found that a primary stage of the well-planned attack involved[17] 'TrickBot', 'AdvisorsBot' and the 'Emotet' multi-functional malware. The notorious 'TrickBot' had partnered with 'IcedID', both banking malware, and machines infected by 'IcedID' had downloaded 'TrickBot' too. In another prominent case, the successful Ramnit 'Black' campaign[18] was observed spreading the Azorult info-stealing malware.

The increase in threat actor collaboration and capabilities expansion marks a great step for cybercriminals, pose a great danger to organizations, and should serve as a reminder that high-profile attacks may be just the first step in a more prolonged operation.

Cloud Risk Trends

2018 introduced a new fertile playground for threat actors—public cloud environments. Containing vast amounts of sensitive data, as well as great computational resources, the cloud has everything a threat actor could dream of. Furthermore, correlating to the increased movement of companies to public cloud services as the main platform for storing and managing their workloads, we witnessed multiple new techniques, tools and exploitations emerging against the cloud this year.

---

[16] https://research.checkpoint.com/emotet-tricky-trojan-git-clones/

[17] http://blog.checkpoint.com/2018/10/23/ransomware-stopped-working-harder-started-working-smarter-botnets-phishing/

[18] https://research.checkpoint.com/new-ramnit-campaign-spreads-azorult-malware/

Nonetheless, the majority of the attacks observed targeting the cloud are mainly derived from poor security measures including misconfigurations and the use of weak credentials which usually involve data compromise and information leakage. This reality essentially leaves so many exposed assets that attackers no longer need exploit a specific vulnerability to gain unauthorized access to sensitive resources. One example, the fitness software company 'Fitmetrix', unfortunately exposed[19] millions of customer records stored in a database hosted on AWS. In another case, personal details of nearly 700,000 American Express[20] India customers were exposed online via an unsecured MongoDB server.

In addition, in 2018 we observed cyber criminals utilizing misconfiguration in the cloud, abusing services hosted there for a wide range of attacks. Among them was performing cryptocurrency mining[21] by leveraging the vast computing power stored in the cloud, enslaving exposed cloud servers to trigger DDoS attacks[22], and even launching man-in-the-middle attacks by exploiting publicly open S3 buckets.

It is therefore safe to say that the bigger the cloud gets, the bigger the target and attention it attracts for cyber criminals. Setting up small environments on public cloud is relatively easy, but when it comes to moving a whole network infrastructure to public cloud, additional security measures must be adopted in order to ensure no asset is left exposed.

Mobile Trends: A Target on Apple's Back

As one of the most prominent actors in the mobile device industry, Apple is considered to have the most secure operating system. Together with keeping this system closed sourced, Apple has multiple built-in security measures aiming to protect their users from a variety of cyber threats. However, some may say that it is not enough.

As Apple's user-base has grown, it has become a more attractive target to threat actors wishing to get their hands on Apple's devices' sensitive data and exploit their tools against them.

---

[19] https://securityaffairs.co/wordpress/77073/data-breach/fitmetrix-data-breach.html

[20] https://securityaffairs.co/wordpress/77815/data-breach/amex-india-data-leak.html

[21] https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/

[22] https://threatpost.com/demonbot-fans-ddos-flames-with-hadoop-enslavement/138597/

During 2018 we witnessed an increase in the number of vulnerabilities exposed for iOS. In one month alone three passcode bypass vulnerabilities[23] were discovered affecting all current iPhone models, including the recently released iOS version 12.0.1, and allowed a potential threat actor to gain access to a user's photos and contacts.

The severe 'Text Bomb'[24] flaw was also found in Apple devices running on iOS and macOS, and was capable of freezing apps and crashing iPhones. Another flaw revealed in 2018 was found in the process of pairing iPhone devices with Mac workstations or laptops, allowing attackers to take over the paired iPhone device without the owners' knowledge.

In addition, traditional malware has now upgraded their capabilities to target iOS devices. The Pegasus Spyware,[25] a cryptocurrency wallet and credential theft malware, and 'Roaming Mantis', a Banking Trojan and cyptocurrency miner[26] disguised as a calendar app, are just few of the threats which managed to breach Apple's Garden Wall and penetrate the App Store last year.

However, these threats are dwarfed by the specially crafted attacks that emerged towards Apple's devices. These include the FallChill malware that utilized a unique Mac function to secretly take screenshots of a victim's phone. This was the first time to see an APT activity,[27] allegedly carried out by the Lazarus Group, targeting OSX devices.

Together with the several high-profile attacks that occurred against Apple itself,[28] it appears then that in 2018 threat actors are now willing to prove that no environment, brand or operation system can be immune against cyber-attacks.

Nation-States: No Longer an Officer and a Gentleman

Cyberspace often provides a veil of secrecy for nation-states to achieve operational gains. Over the past years, however, a trend has emerged to indicate that several have given up this veil and now operate quite openly, almost provocatively. Indeed, national interests are continuously exposed, with unrestrained demonstration of offensive capabilities. Of course, while no country takes responsibility for cyber-attacks, attribution is sometimes not too difficult to assign.

The precedents for such openness can be found in the aggressive Russian attacks against the Ukraine. Black Energy, which took down the power grid[29] in Ukraine in 2015 and NotPetya[30] which shut down the entire country in 2017, marked the way for several more countries to operate more freely; sometimes without the use of evasion techniques or fully covering their tracks.

---

[23] https://thehackernews.com/2018/10/iphone-lock-passcode-bypass.html

[24] https://threatpost.com/apple-rushes-fix-for-latest-text-bomb-bug-as-abuse-spreads/129987/

[25] https://thehackernews.com/2018/09/android-ios-hacking-tool.html

[26] https://arstechnica.com/information-technology/2018/03/theres-a-currency-miner-in-the-mac-app-store-and-apple-seems-ok-with-it/

[27] https://securelist.com/operation-applejeus/87553/

[28] https://www.welivesecurity.com/2018/08/17/australian-schoolboy-apples-network/

[29] https://www.bankinfosecurity.com/ukrainian-power-grid-hacked-a-8779

[30] https://www.cnet.com/news/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/

The infamous North Korean hacking group, Lazarus, was considered responsible for numerous violent attacks over the last year and before too. Indeed, with the devastating WannaCry attack, the Sony hack,[31] SWIFT banking theft[32] and the hacking of Cryptocurrency Exchanges,[33] North Korea abandoned elegance in 2018 and marched to a far more aggressive approach.

Iran was also demonstrating evolving cyber capabilities in the cyber espionage arena in 2018. As illustrated by Check Point Research, Iran's Domestic Kitten[34] campaign was aimed towards international elements as well as against its own citizens to serve its national interests, utilizing both mobile and desktop attack vectors to achieve its goals. With Domestic Kitten, Iran managed to carry an extensive surveillance campaign through mobile apps for years, and with Charming Kitten, an additional Iranian group, it joined a long list of espionage campaigns against Western and academic targets, using spear phishing emails.[35] Again, it put minor efforts in hiding their operations.

Alongside intelligence goals like espionage or surveillance campaigns, nation state cyber attacks exposed some new missions such as sabotage, financial gains and revenge. Such was arguably the case with 'Olympic Destroyer' which threatened to ruin the Winter Olympic Games[36] in South Korea this year. While no attribution has yet been confirmed, considering the above trend it may not be too difficult to hazard a guess as to who the perpetrator might be. While the West retains a degree of statehood in cyberspace, there are nation-states, mainly eastern ones, who appear to be acting unbridled in their own interests.

---

[31] https://securityaffairs.co/wordpress/75994/cyber-warfare-2/north-korea-agent-indictment.html

[32] https://securityaffairs.co/wordpress/78382/apt/lazarus-latin-american-banks.html

[33] https://securityaffairs.co/wordpress/77213/hacking/cyber-attacks-crypto-exchanges.html

[34] https://research.checkpoint.com/domestic-kitten-an-iranian-surveillance-operation/

[35] https://threatpost.com/charming-kitten-iranian-2fa/139979/

[36] https://www.theguardian.com/sport/2018/feb/11/winter-olympics-was-hit-by-cyber-attack-officials-confirm,%20 http:/blog.talosintelligence.com/2018/02/olympic-destroyer.html

PAST: REVIEW OF 2017 PREDICTIONS

In last year's Security Report we predicted where each information systems platform was headed in 2018. To compare, we have revisited those predictions to see how they fared over the past twelve months.

Mobile

We expected that flaws in mobile operating systems and technology would continue to be discovered and this was very much the case. As seen by our discovery of vulnerabilities that reside in the default keyboard on all mainstream LG smartphone models, which account for over 20% of the Android OEM market[37] in the US, flaws such as these leave the door open to attackers carrying out Remote Code Injection attacks to spread malware.

In addition, flaws were found by Check Point Research in the Android operating system itself, leaving the External Storage component on devices worldwide exposed to a Man-in-the-Disk attack. Despite app developers being provided with guidelines on how they can avoid leaving their applications vulnerable, it is well known that developers do not have security front of mind when creating such apps. Operating system providers also do not do enough to ensure their devices are protected. As a result, the need remains for organizations to deploy advanced protection against mobile malware and interception of communications.

Mobile malware continued to proliferate too, as seen by up to seven million users who downloaded the AdultSwine[38] malware that infected over 60 children's game apps and exposed them to inappropriate ad content. RottenSys[39], a mobile adware, infected over five million devices with adware since 2016. Also, cryptominers entered the threat landscape not only on PCs and web servers, but across five billion mobile devices in use around the globe.

Cloud

Not surprisingly, and as expected, the theft of data stored on the cloud continued to plague organizations of all sizes as they transitioned their infrastructures to this cost-effective and agile platform. From fitness apps like Under Armour and PumpUp to retailers and ticket box office companies like TicketFly, not to mention Facebook, data breaches occurred on a daily basis and will continue to do so across all industries due to the value they hold for cyber criminals.

---

[37] https://phandroid.com/2017/05/08/lg-market-share-q1-2017/

[38] https://research.checkpoint.com/malware-displaying-porn-ads-discovered-in-game-apps-on-google-play/

[39] https://research.checkpoint.com/rottensys-not-secure-wi-fi-service/

In addition, the introduction of GDPR last year added extra stress and pressure to those who hold customer data not only in the cloud but on their organization's servers in general. It's understood that these new regulations carry hefty fines for those who do not comply.

For this reason, we encourage all our customers to take the Shared Responsibility model seriously and not rely solely on their cloud provider's basic protections to keep them safe from known and unknown threats.

Network

Last year we predicted that ransomware 'refer a friend' schemes would surface. While those programs have yet to be seen, what *is* prevalent, as predicted in last year's report, is the Ransomware-as-a-Services now being offered through affiliate programs on the Dark Web. These programs advertise themselves to technically low-level threat actors wanting to get in on the action at a low cost.

In addition, while cryptominers entered network servers to harness the large CPU power they offer, ransomware attacks have not disappeared. WannaCry, the mega attack of 2017 with suspected North Korean origins, was responsible for attacks on Boeing's IT systems last year and it could be adapted to function as a cryptominer in the future.

After all, worms like ransomware that infect networks never really die out. Indeed, we are still seeing worms like Conficker from 2009 and traces of SQLSlammer from 2003 still in circulation.

IoT

Following our report into the ways threat actors could invade the privacy of consumers' homes via IoT devices such as vacuum cleaners, our prediction came true that these same types of exploits could well be applied to enterprise organizations' use of IoT devices

Through the discovery of vulnerabilities in DJI drones, the manufacturer of choice for 70% of the worldwide drone market, we revealed how gaps in the security of these devices can expose enterprises to great damage. Threat actors are presented with an opportunity to view and steal sensitive information of critical infrastructure, for example, collected by the drone and could be used in a future attack.

It's still the case that users are generally not aware of the security element of their IoT devices, and tend to leave the default settings in their original state. This continues to leave the door wide open for attackers to gain access to a consumer or organization's IT network.

Cryptocurrencies

Despite our expectation, digital currencies are still not heavily regulated. For this reason, we continue to see cryptocurrencies as the payment method of choice for cybercriminals behind ransomware attacks, and as an incentive for crypto-mining malware.

What began as a relatively new malware at the end of 2017 became the new norm in 2018. Our predication as detailed in this report was right on.

In addition, our forecast that the value of these currencies would drop also came to pass although we thought it would be due to intervention of international government and law enforcement agencies. Instead, it was the increase of attacks on cryptocurrency exchanges themselves, such as those seen on Bithumb, Coinrail and CoinCheck. As we predicted, this sent shockwaves through the lucrative digital industry. In turn, this made investors nervous and dramatically lowered the value of Bitcoin, among others.

CONCLUSION: NEXT STEPS

As we have seen, the attacks of 2018 are characterized as being more targeted and stealth like. Whether carried out by cyber criminals or nation-states, these attacks reveal interesting new trends and motivations. From cryptomining to ransomware, mobile device vulnerabilities to attacks for the sake of national interests, all have made a significant impact on today's threat landscape.

Whereas we saw cryptominers taking a central role in infecting organizations, with over 40% of organizations subject to cryptomining attempts in the past year, making it the most prevalent malware type, ransomware became directed at more specific targets. These included municipal IT infrastructures, hospitals, seaports and airports, newspapers and many other undisclosed institutions.

Malware also became more multi-functional in its methodology and purposes, generating hybrid assaults that combined cryptominers, banking malware and botnet attempts. Previously considered a "walled garden", 2018 also saw an increase in the number of successful attacks on the previously considered safe mobile operating systems.

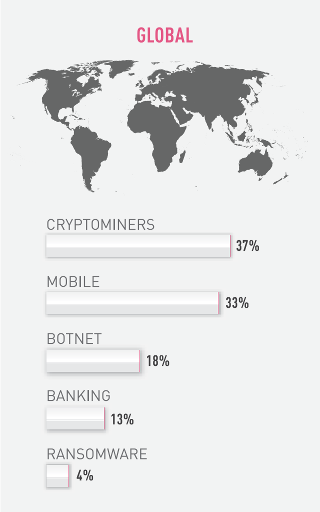
As a result, and to provide organizations with the best level of protection, IT security professionals must be attuned to the ever-changing landscape and the latest threats and attack methods.

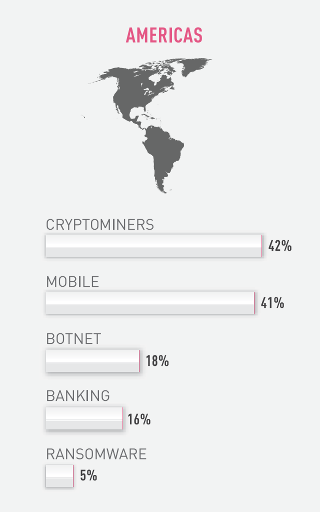
In the next installment of this Security Report we will take a deeper look under the hood of today's Malware-as-a-Service industry sold on the Dark Net, providing even inexperienced attackers access to sophisticated cyber weapons. As we will see, in 2018, this was more widespread than ever before as cyber crime has now become democratized.

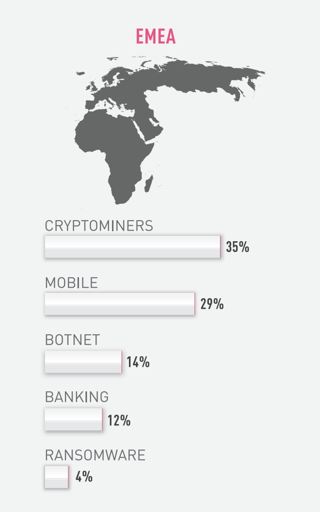
INDEX: 2018's TOP MALWARE FAMILIES

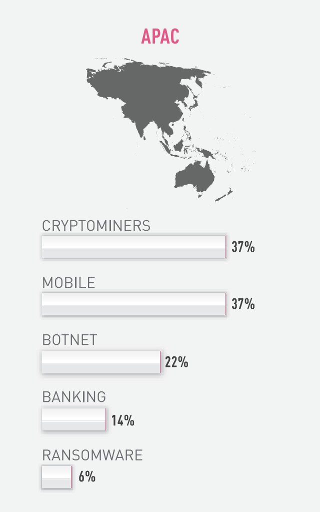
Cyber Attack Categories by Region

Looking back at our charts from 2017 and 2018, a great transformation can be observed. Ransomware is no longer on the top of the malware list. In fact, the general impact of ransomware over organizations world-wide dropped from 30% at its peak in 2017 to less than just 4% in 2018. This shift may be the result of the move to cryptomining as a more efficient and profitable alternative. It can also be related to the adoption of the 'boutique' ransomware attacks that only target specific organizations instead of wide global campaigns.

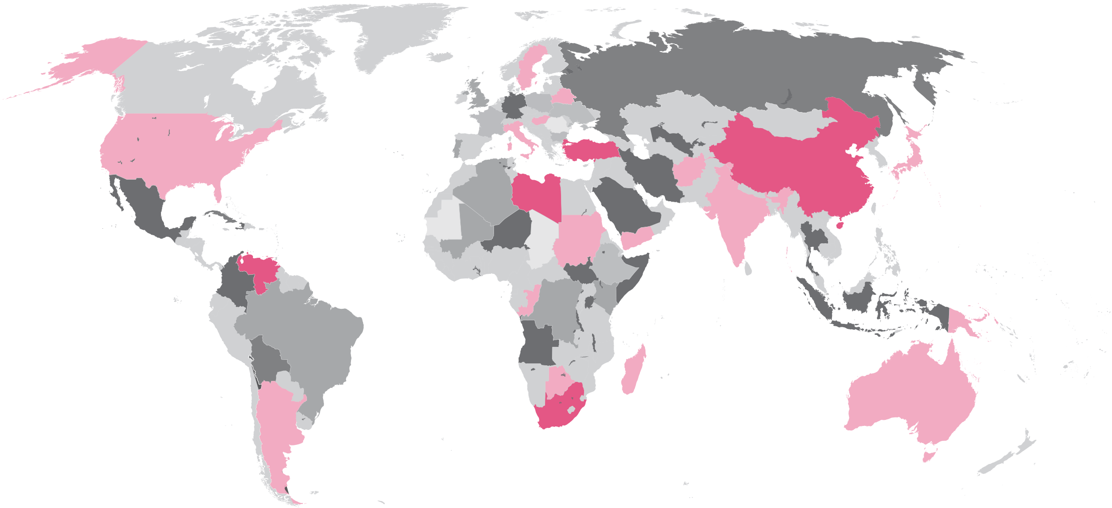

GLOBAL

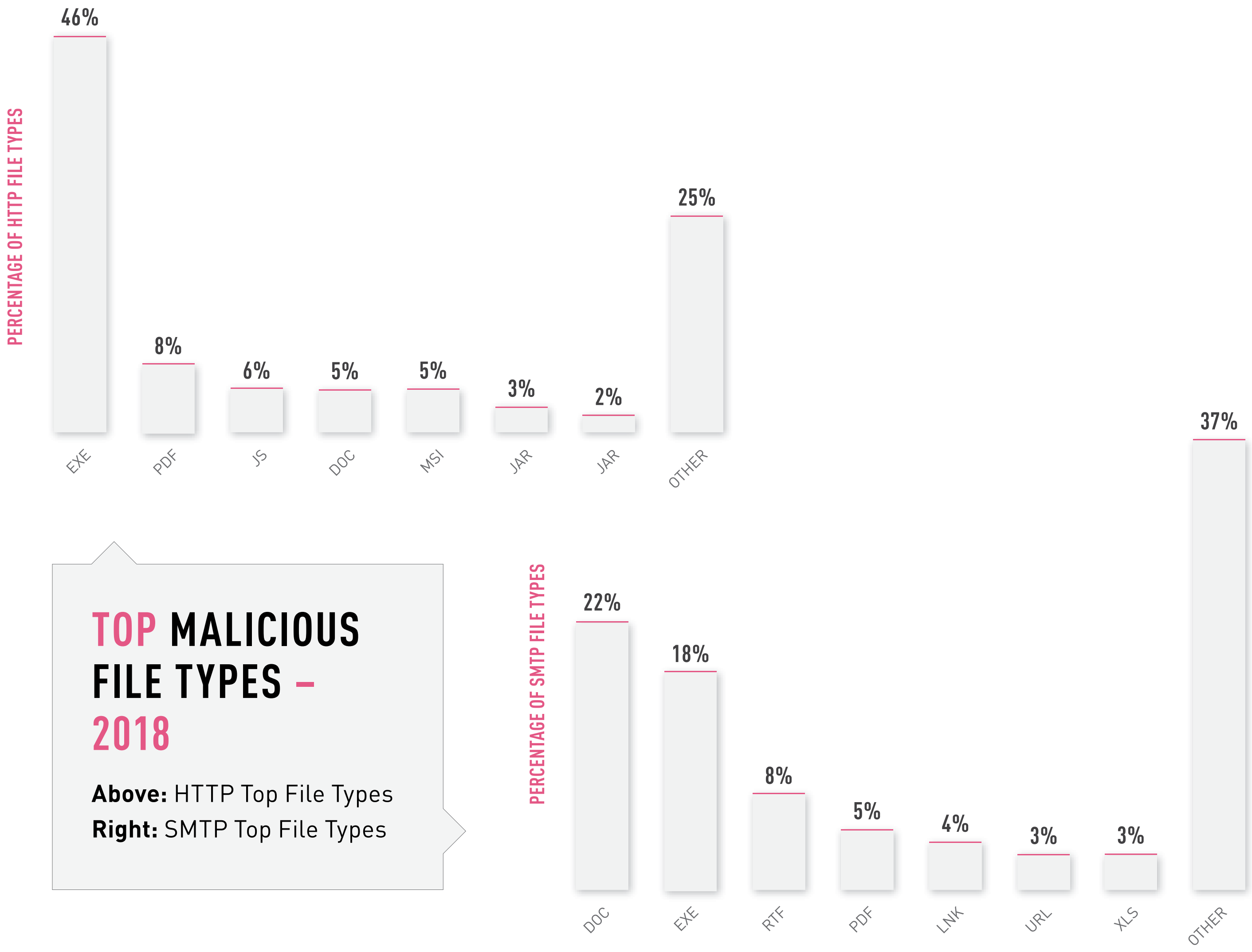

AMERICAS


EMEA


APAC

Global Threat Index Map

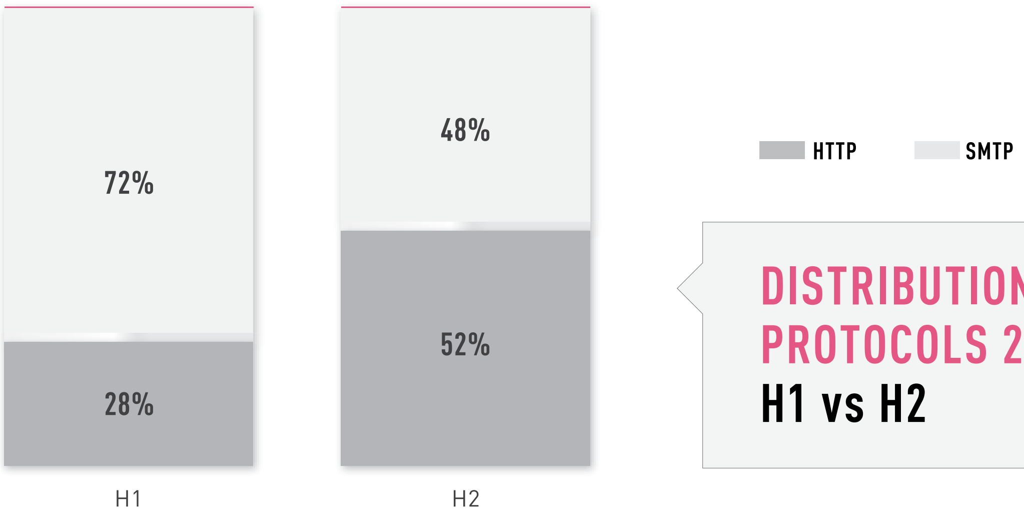




TOP MALICIOUS FILE TYPES – 2018

Above: HTTP Top File Types

Right: SMTP Top File Types



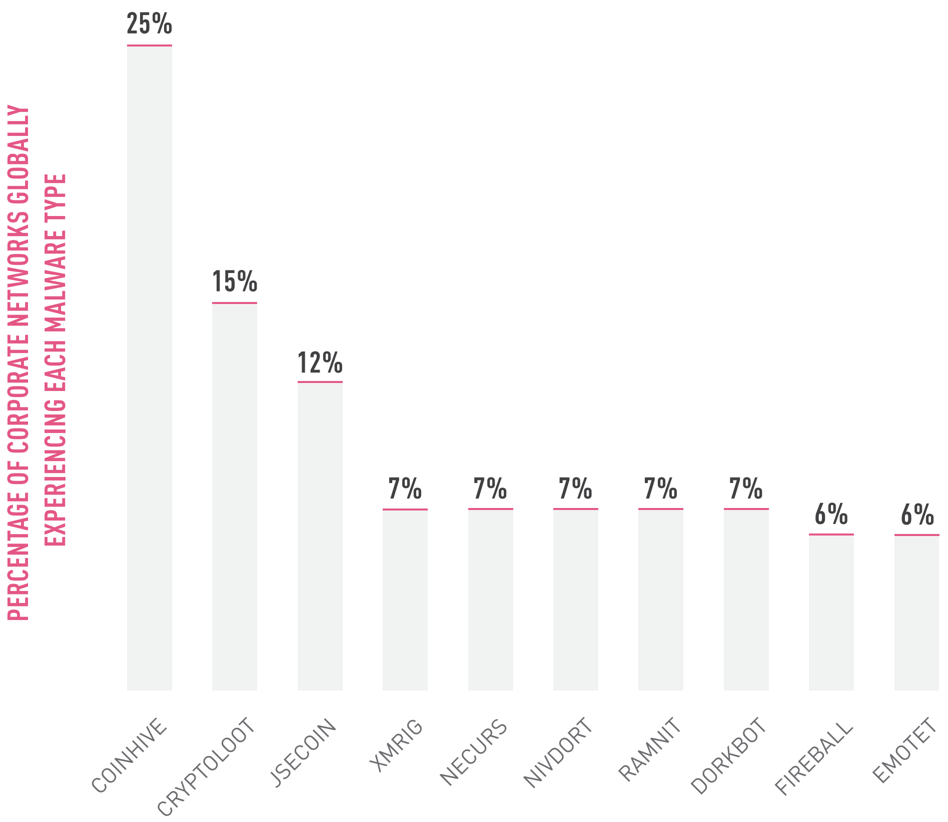
DISTRIBUTION PROTOCOLS 2018 H1 vs H2

APPENDIX A: TOP MALWARE FAMILIES

Global Malware Statistics

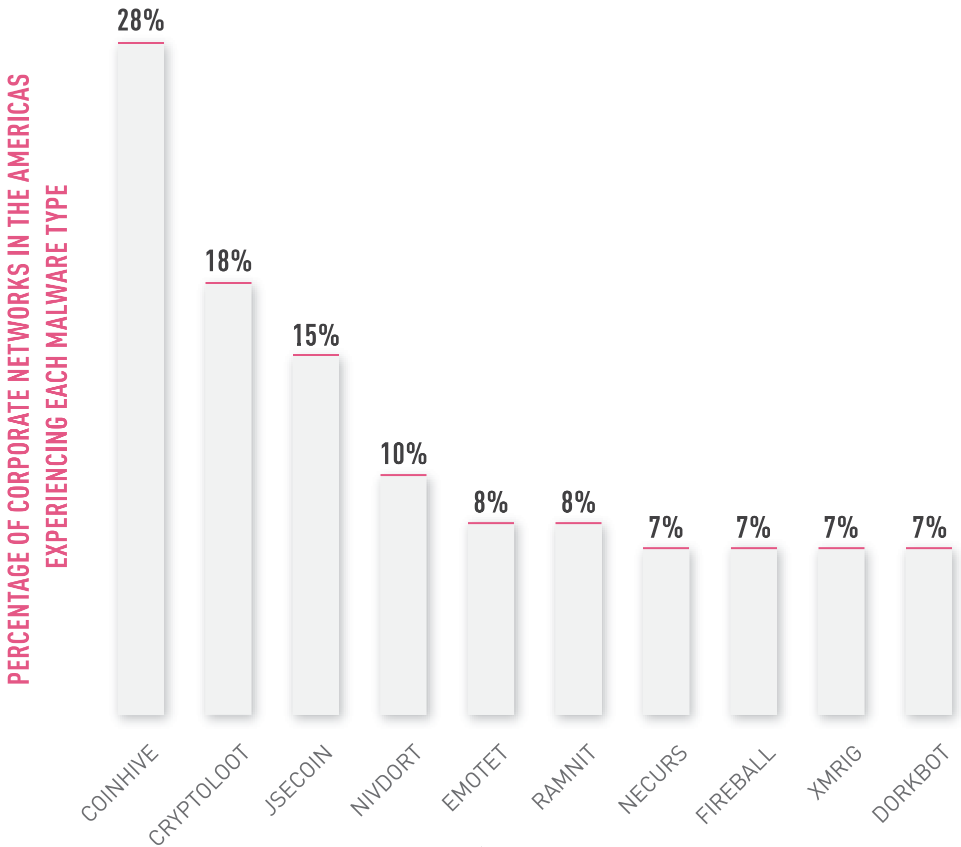
Data comparisons presented in the following sections are based on data drawn from the Check Point ThreatCloud Cyber Threat Map between January and December 2018.

For each of the regions below we present two graphs. The first details the most prevalent malware in that region, followed by a second graph that details the malware families with the highest presence in that region compared to others.



TOP GLOBAL MALWARE FAMILIES

Figure 1: Most Prevalent Malware Globally: Percentage of corporate networks experiencing each malware type



TOP MALWARE FAMILIES IN **AMERICAS**

Figure 2: Most Prevalent Malware in the Americas

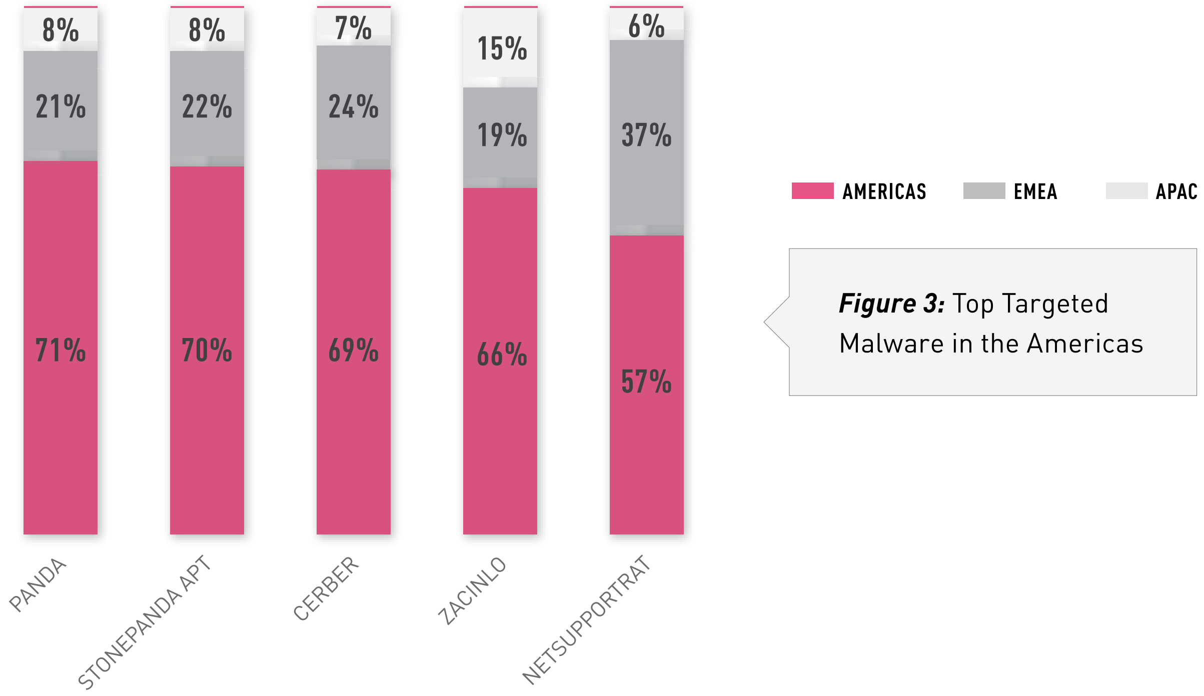
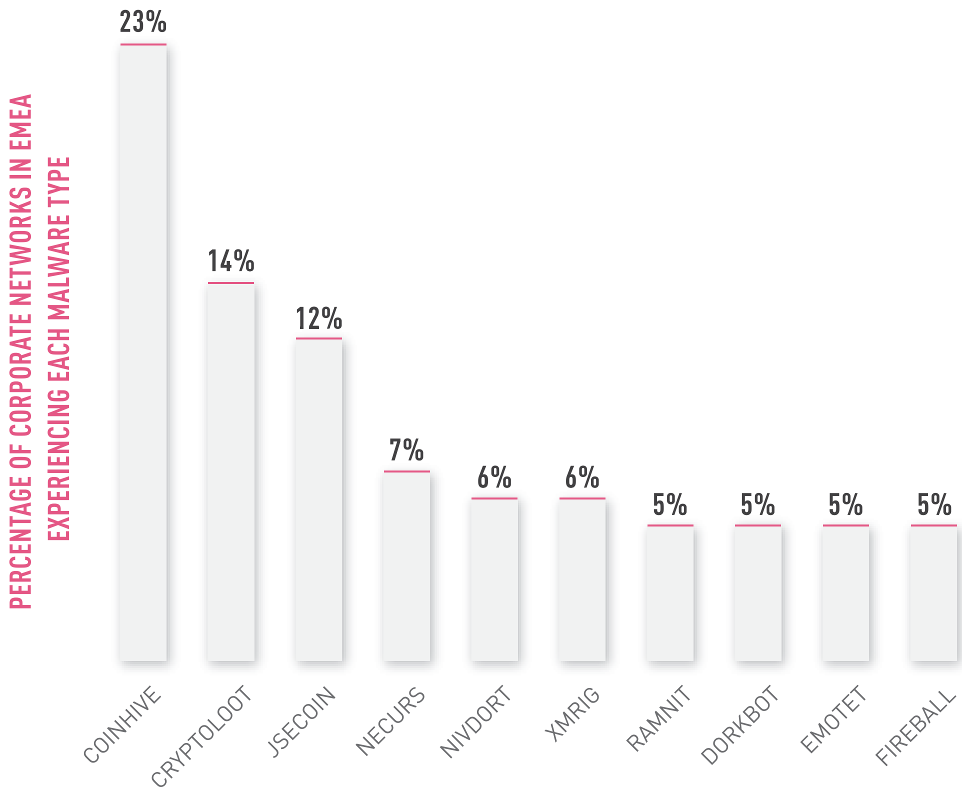


Figure 3: Top Targeted Malware in the Americas



TOP MALWARE FAMILIES IN **EMEA**

Figure 4: Most Prevalent Malware in the EMEA

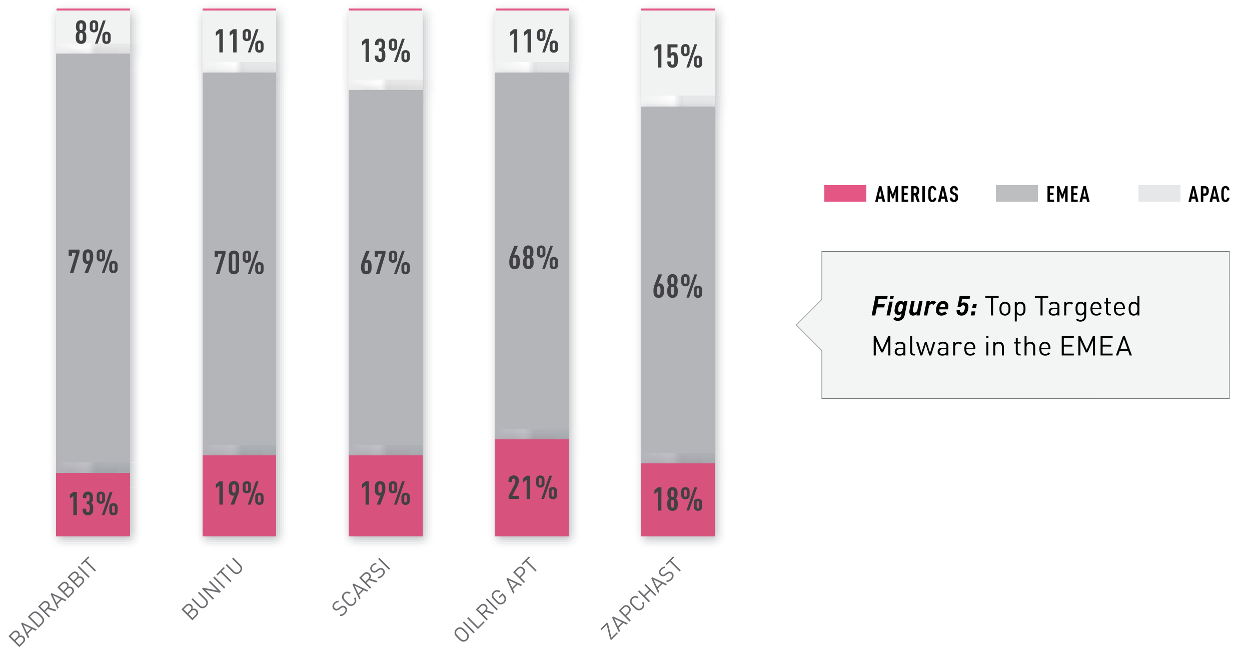
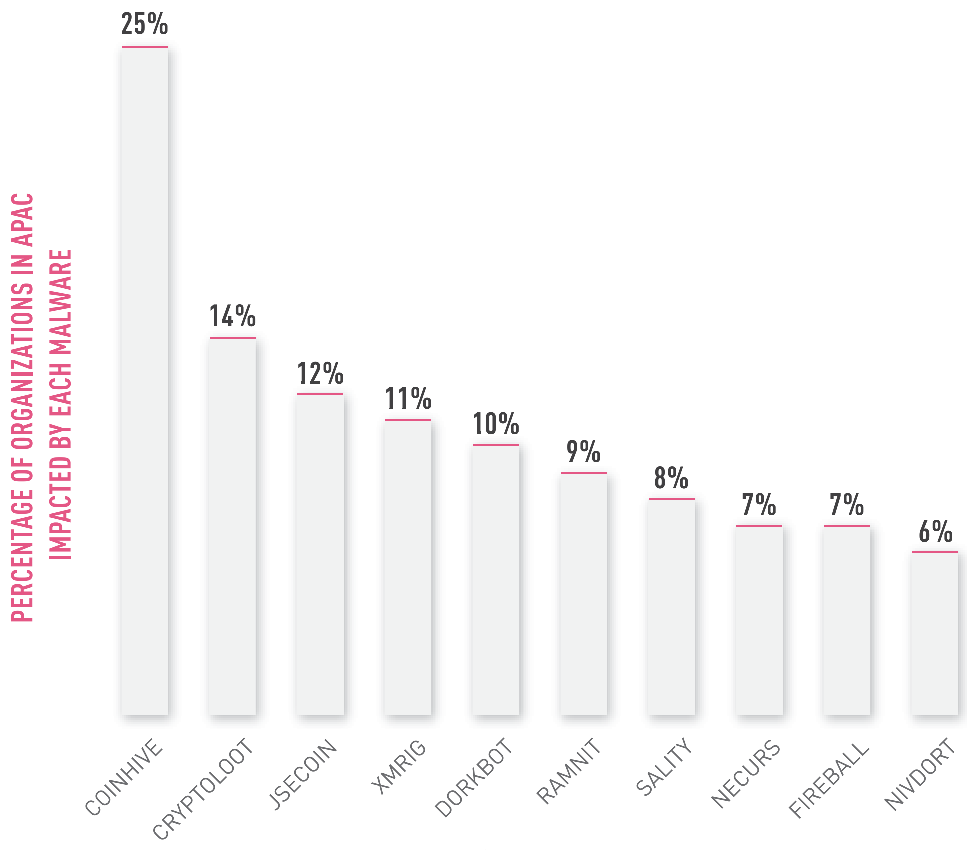


Figure 5: Top Targeted Malware in the EMEA



TOP MALWARE FAMILIES IN **APAC**

Figure 6: Most Prevalent Malware in the APAC

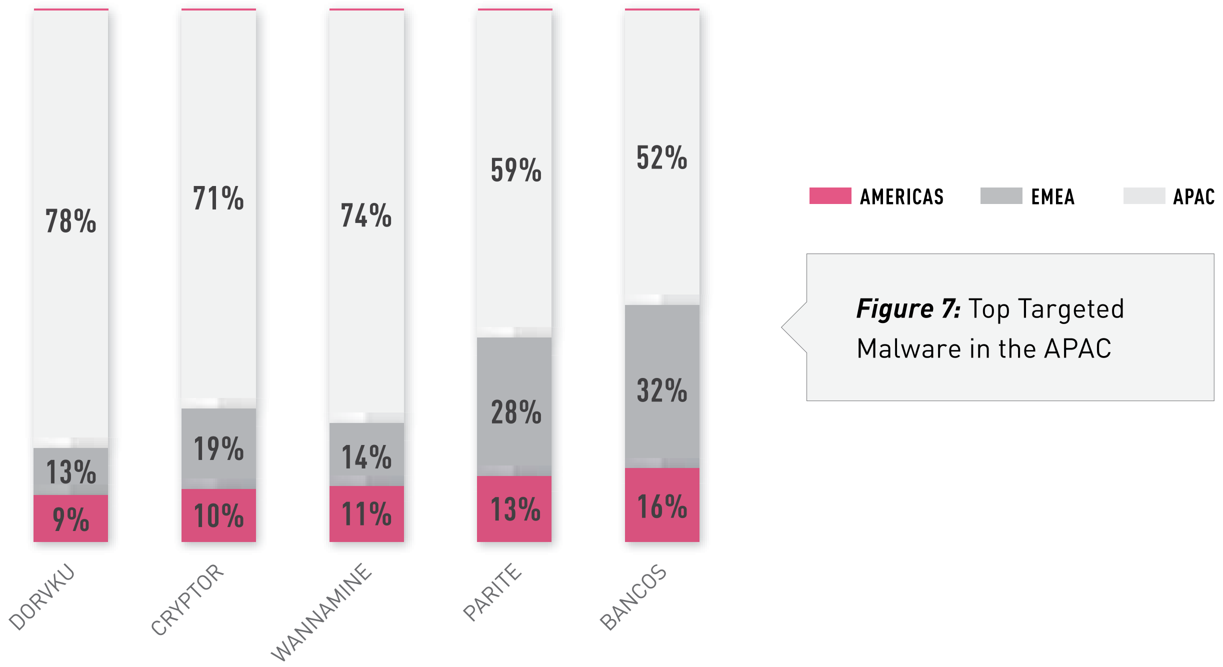


Figure 7: Top Targeted Malware in the APAC

Global Analysis of Top Malware

Coinhive, the prominent web-based Monero Cryptocurrency miner, has yet again maintained its place at the top of our global malware rank, with 25% of the organizations worldwide affected. Coinhive is delivered via YouTube[40] and Google's DoubleClick[41] advertisements and Facebook Messenger, as well as embedded in tens of thousands of websites. Our global top malware charts for both parts of 2018 show that cryptomining malware is officially the most prominent malware type of the year, with a global impact of nearly 40%.

Emotet, one of the most prominent Trojans in the wild, has climbed its way to the top of global and the Americas top rankings. As an advanced, self-propagating and modular Trojan, Emotet, once employed as a banker, is distributed in massive spear-phishing campaigns together with malicious links or attachments. One of these was a Thanksgiving-themed campaign[42].

---

[40] https://www.bleepingcomputer.com/news/security/coinhive-cryptojacker-deployed-on-youtube-via-google-ads/

[41] https://blog.trendmicro.com/trendlabs-security-intelligence/malvertising-campaign-abuses-googles-doubleclick-to-deliver-cryptocurrency-miners/

[42] https://www.forcepoint.com/blog/security-labs/thanks-giving-emotet

Top Cryptomining Malware

The following charts show the percentage of organizations that were affected by each cryptomining malware, and provide global views and regional insights.

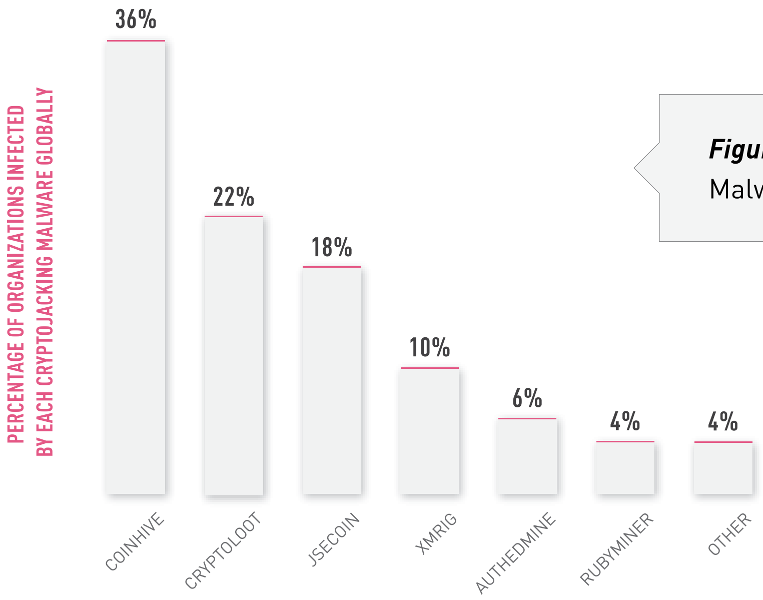


Figure 8: Top Cryptomining Malware **Global**

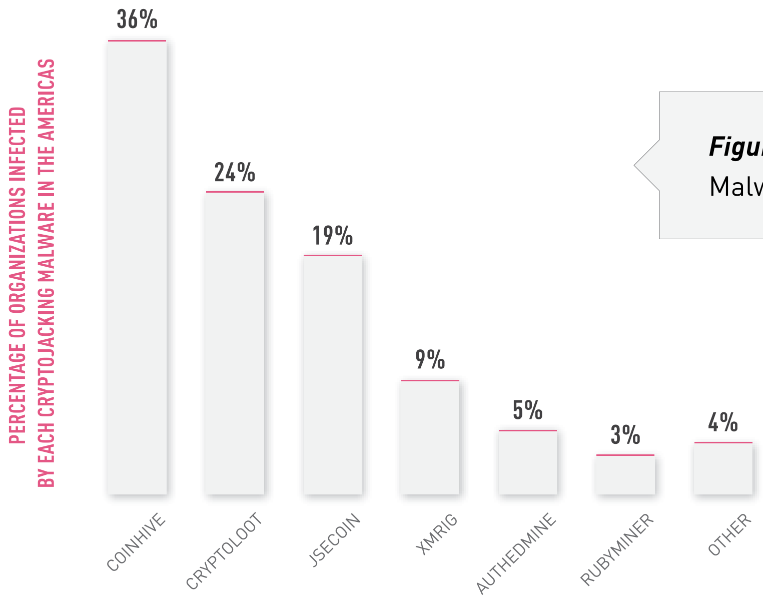


Figure 9: Top Cryptomining Malware **Americas**

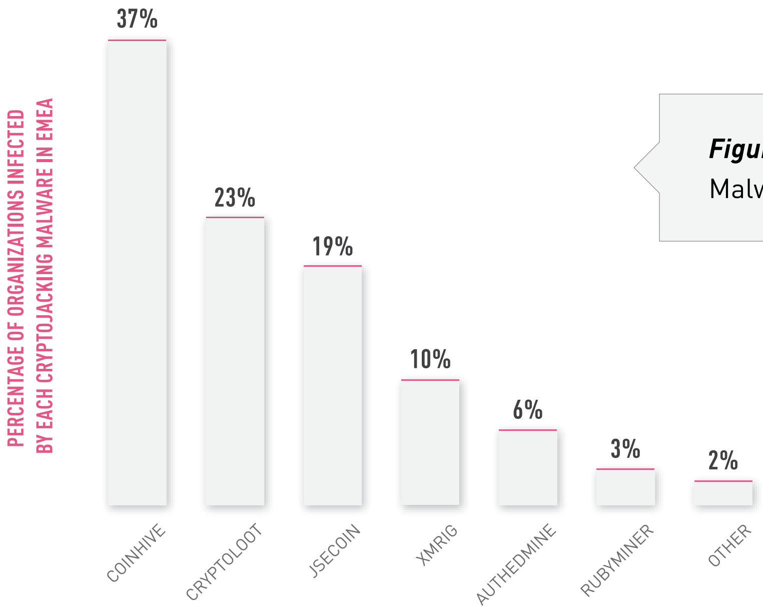


Figure 10: Top Cryptomining Malware **EMEA**

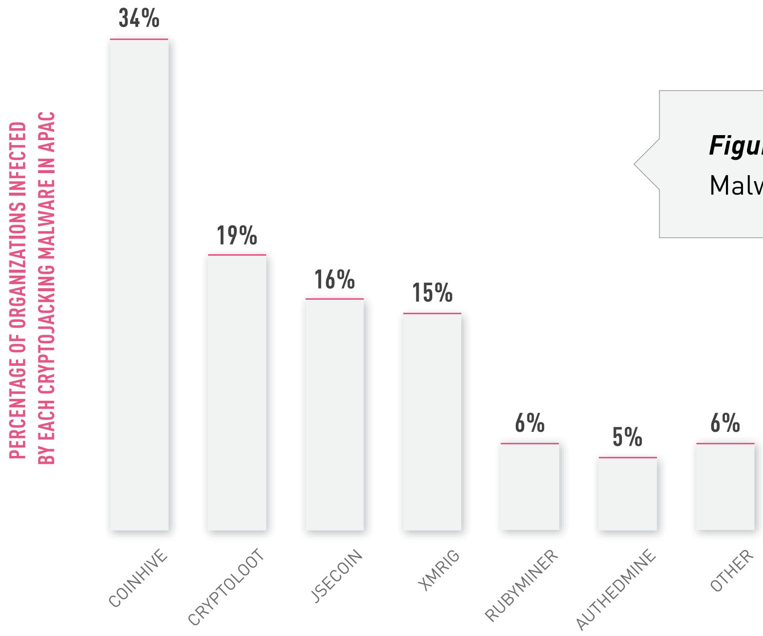


Figure 11: Top Cryptomining Malware **APAC**

Cryptominers Global Analysis

The most prominent cryptomining malware dominating the Global Top Cryptominers Malware list, Coinhive, Cryptoloot and JSEcoin, have kept their place at the top of the list since 2017. These popular web-based cryptominers are easily integrated into websites—willingly by website owners as well as unknowingly by threat actors who utilize the websites' high traffic. Taking a different approach, the RubyMiner campaign targeted unpatched Windows and Linux servers, and maintained its high rank during the first half of 2018. As revealed by Check Point researchers[43] last January, RubyMiner attempted to exploit 30% of all corporate networks worldwide to mobilize powerful servers into its operators' mining pool.

---

[43] https://research.checkpoint.com/rubyminer-cryptominer-affects-30-ww-networks/

Top Banking Trojans

In this section, we show the percentage of organizations that were affected by each banking malware and provide global views and regional insights.

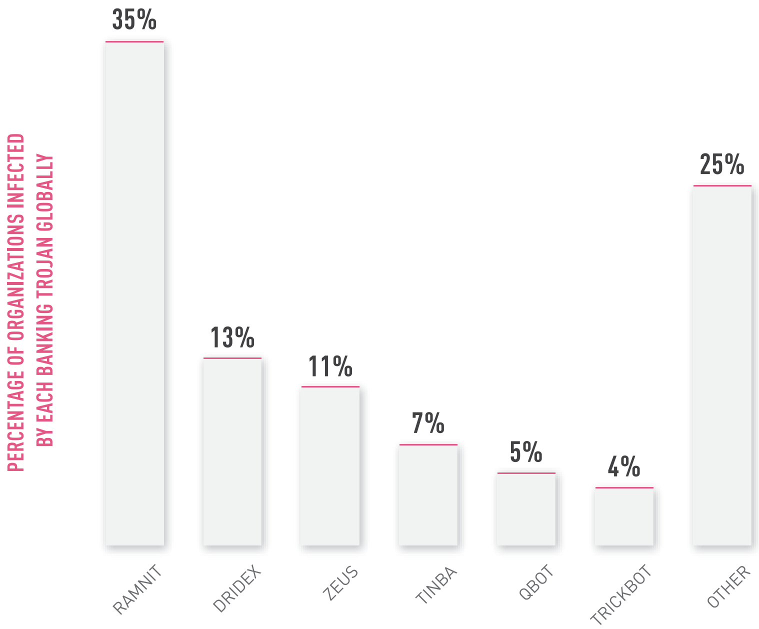


Figure 12: Top Banking Trojans **Global**

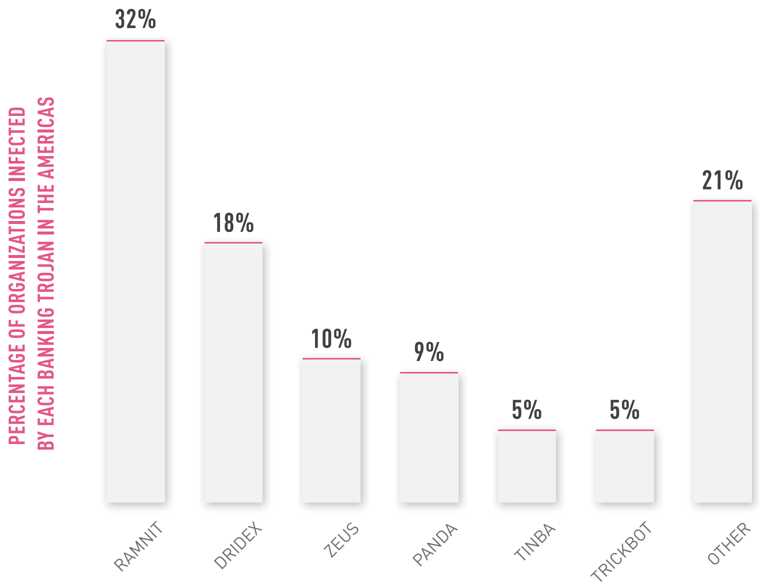


Figure 13: Top Banking Trojans **Americas**

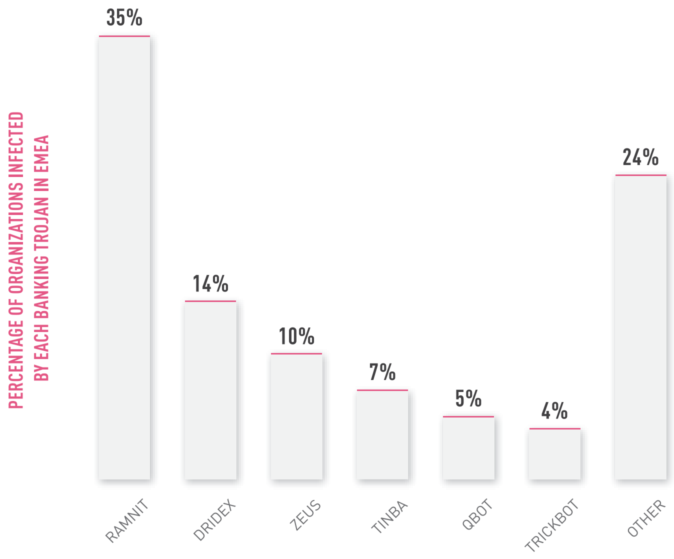
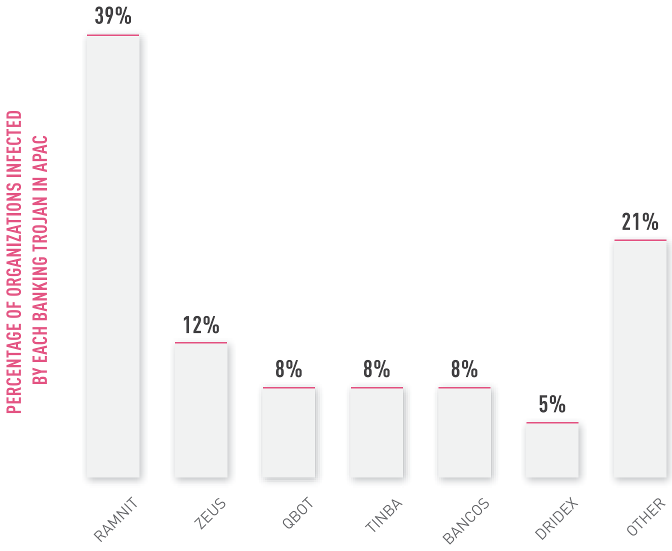


Figure 14: Top Banking Trojans **EMEA**

Figure 15: Top Banking Trojans **APAC**



Banking Malware Global Analysis

Ramnit is the most prominent banking Trojan of the past year. It first appeared in 2010 and has remained active ever since. Ramnit's popularity is in line with the exposure by Check Point researchers of a massive new 'Black' campaign[44] based on the banker. The campaign turned the victim machines into malicious proxy servers and resulted in over 100,000 infections. Shortly after the 'Black' campaign was shut down, a new Ramnit campaign emerged, distributing[45] the AZORult info-stealer and downloader, via the RIG and GrandSoft Exploit Kits.

Trickbot is another dominant banking Trojan widely observed in 2018 that reached the top of the global, Americas and EMEA rankings. As an advanced malware based on plugins, Trickbot is constantly being updated[46] with new capabilities, features and distribution vectors. This enables Trickbot to be a flexible and customizable malware that can be distributed as part of multi-purposed campaigns. This year we witnessed TrickBot being delivered[47] via multiple global spam campaigns, as well as creatively cooperating[48] and sharing profits with the IcedID banking malware.

---

[44] https://research.checkpoint.com/ramnits-network-proxy-servers/

[45] https://research.checkpoint.com/new-ramnit-campaign-spreads-azorult-malware/

[46] https://www.webroot.com/blog/2018/03/21/trickbot-banking-trojan-adapts-new-module/

[47] https://myonlinesecurity.co.uk/trickbot-via-fake-lloyds-bank-important-please-review-attached-documents/

[48] https://www.flashpoint-intel.com/blog/trickbot-icedid-collaborate-increase-impact/

Top Botnet Malware

The following charts show the percentage of organizations that were affected by each Botnet and provide global views and regional insights.

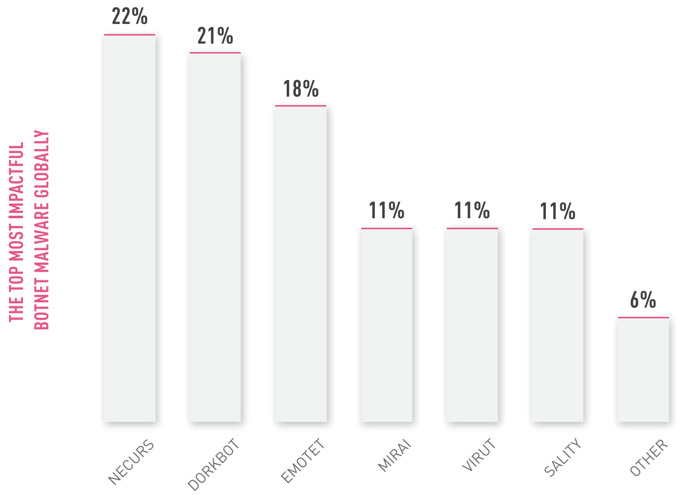


Figure 16: Top Botnet Malware **Global**

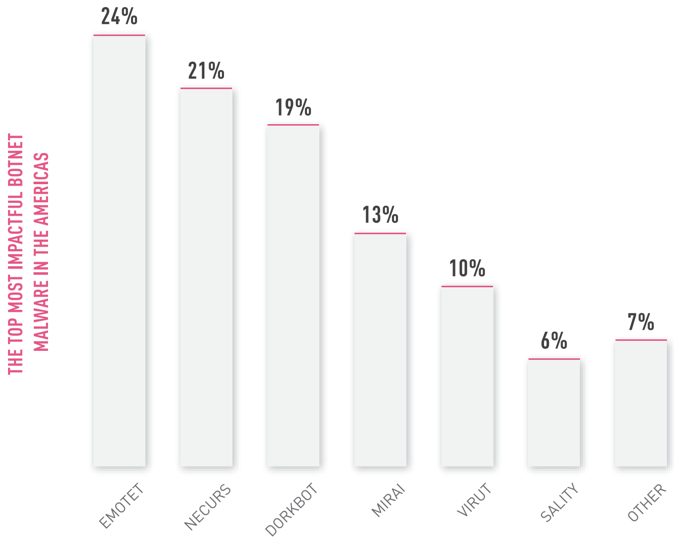


Figure 17: Top Botnet Malware **Americas**

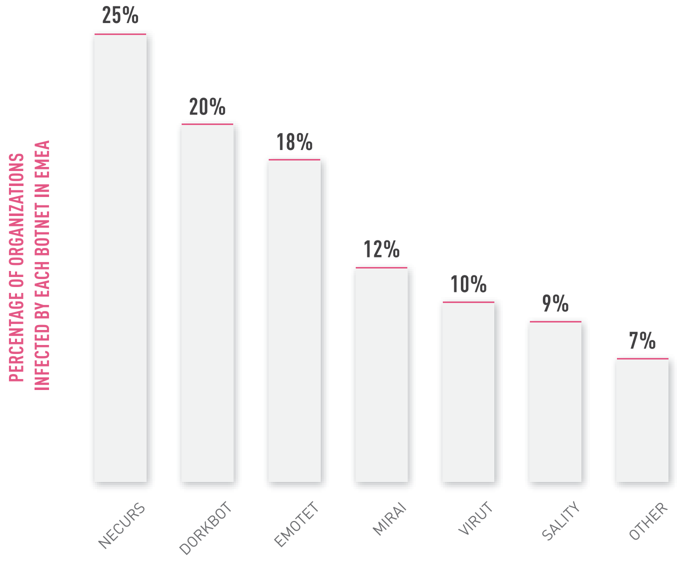


Figure 18: Top Botnet Malware **EMEA**

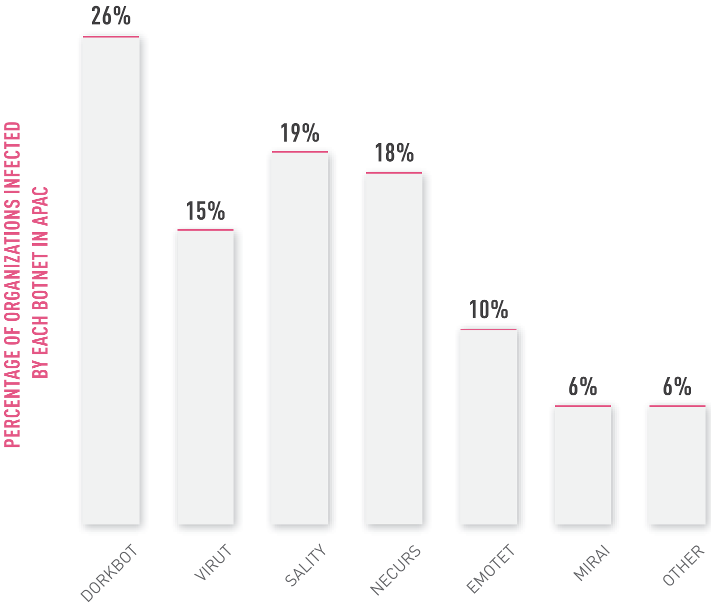


Figure 19: Top Banking Trojans **EMEA**

Botnet Malware Global Analysis

The notorious Necurs, which first emerged in 2012, is at the head of the top global, Americas and EMEA ranks, and is one of the most prevalent botnets of 2018. This year, the giant spam botnet adopted new techniques to avoid detection, targeted banks,[49] was behind a variety of email scams,[50] and pushed various payloads including cryptominers, ransomware, banking Trojans, and RATs. Due to its massive distribution size, 'Necurs' was single-handedly responsible for the steep rise we observed in URL file type,[51] using it to trick victims into clicking and downloading an additional malware.

Dorkbot is another prominent botnet which dominated the charts. It reached the top of APAC ranks, and also ranked second in the EMEA and globally. Dorkbot, the known modular bot which functions mainly as a downloader or as a launcher for other binary components, was observed this year utilizing an array of Anti-VM and persistence techniques, as well as APC-Injection which allows it to inject malicious code into a legitimate process in a very early stage of thread initialization, thus avoiding detection.

According to our sensors, Andromeda botnet also reached the top of the ranking lists with numerous infected PCs, even though it has been more than a year since its takedown. It appears that traces of the Andromeda botnet remained active in many devices. However, as it lacks the ability to retrieve or carry out commands, we decided not to include it in the threat landscape review.

---

[49] https://www.securityweek.com/necurs-campaign-targets-banks?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29

[50] httphttps://www.bleepingcomputer.com/news/security/necurs-botnet-distributing-sextortion-email-scams/

[51] https://blog.trendmicro.com/trendlabs-security-intelligence/necurs-evolves-to-evade-spam-detection-via-internet-shortcut-file/

Top Mobile Malware

The following charts show the percentage of organizations that were affected by each mobile malware and provide global views and regional insights.

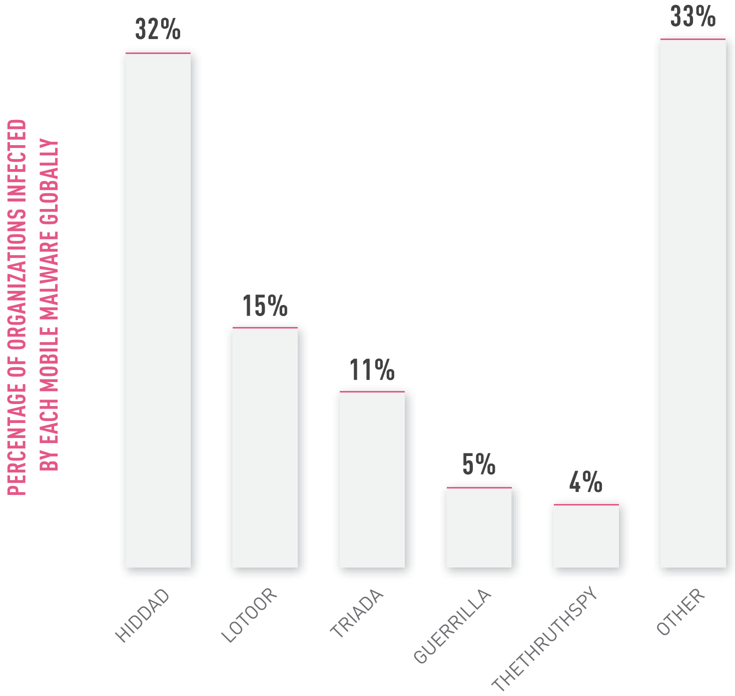


Figure 20: Top Mobile Malware **Global**

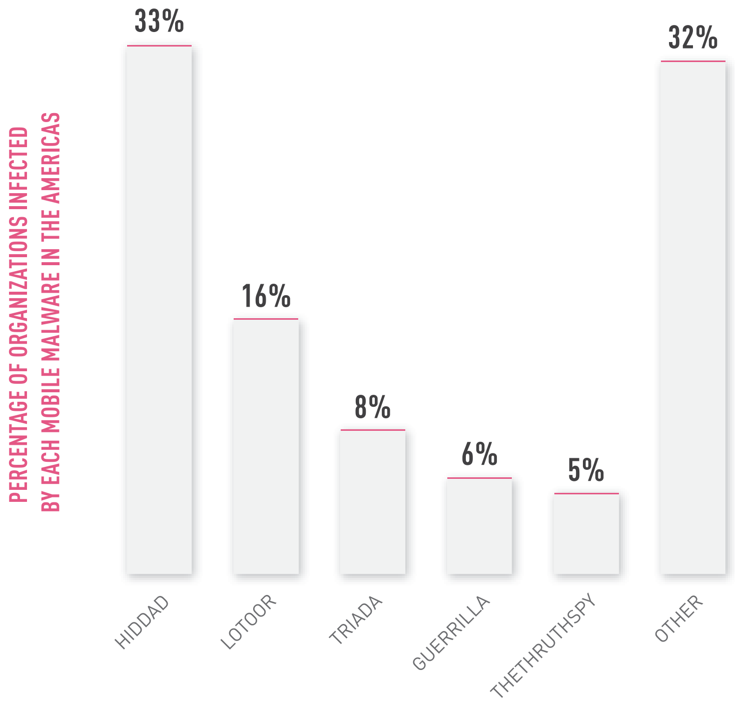


Figure 21: Top Mobile Malware **Americas**

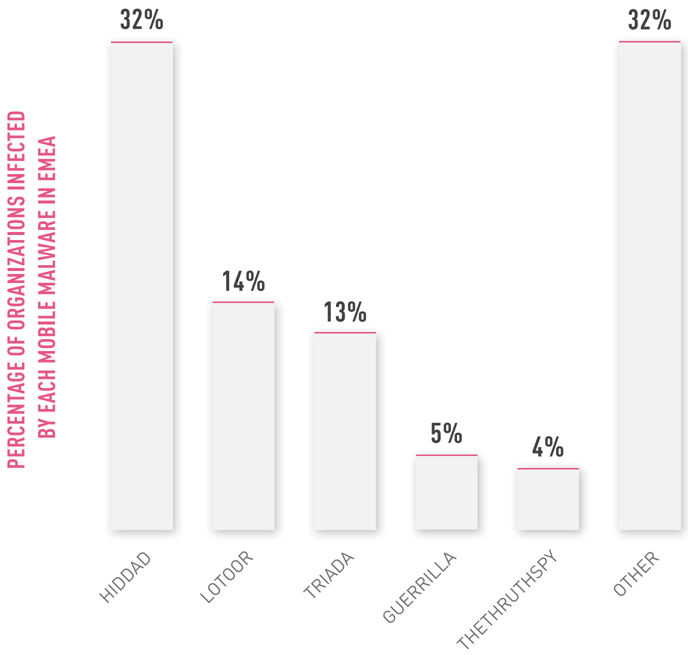


Figure 22: Top Mobile Malware **EMEA**

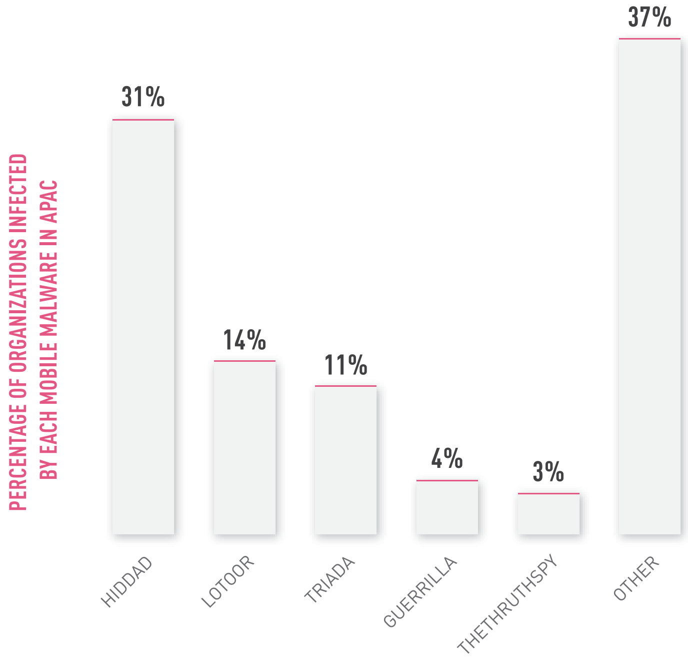


Figure 23: Top Mobile Malware **APAC**

Mobile Malware Global Analysis

Hiddad, an ad-distributing malware for Android that can bypass the Google Play Protect verification system, is back in the top ranks as the top mobile malware globally, as well as in the APAC and EMEA. This year Hiddad presented various persistence techniques[52] along with camouflage methods[53], which made it one of the most prominent mobile malware in the wild.

Guerilla is a new mobile malware family which is embedded in multiple legitimate apps and can download additional malicious payloads to generate fraudulent ad revenue.

---

[52] https://blogs.quickheal.com/aware-hiddad-malware-present-google-play-store/

[53] https://blog.avira.com/top-rated-android-malware/

APPENDIX B: GLOBAL TOP EXPLOITED VULNERABILITIES

The following list of top attacks is based on data collected by the Check Point Intrusion Prevention System (IPS) solution and details some of the most popular and interesting attack techniques and exploits observed by Check Point researchers in the second half of 2018.

Oracle WebLogic Server (CVE-2017-10271)

A proof of concept published in December 2017, led to a high volume of malicious activity associated with the exploitation of the Oracle WebLogic Server Remote Code Execution vulnerability, which allows attackers to remotely execute arbitrary code. Threat actors have since adopted this vulnerability in a wide range of attacks including cryptocurrency miners[54] on unpatched servers[55] and the Satan Ransomware[56] variant, which targeted the US government payment portals[57] with a Trojan to harvest credit cards details.

Apache Struts 2 vulnerabilities (CVE-2017-5638, CVE-2018-11776)

The first Apache Struts vulnerability made headlines in 2017, when attackers exploited it to target the popular financial services provider ‘Equifax’[58] and compromised the sensitive information of over 148 million individuals in the US, UK and Canada. The vulnerability was used to create a maliciously crafted request to an Apache web server to gain access to client hosts and was featured this year in campaigns delivering cryptominers[59] and also the infamous Mirai botnet.[60] In addition, new critical remote code execution vulnerability in Apache Struts 2 was discovered in August, and was soon in use in the wild to spread a cryptomining malware dubbed “CNRig”.[61]

Drupalgeddon2 and Drupalgeddon3 (CVE-2018-7600, CVE-2018-7602)

The highly critical flaws in Drupal, the Content Management System (CMS) giant, were two of the most prominent vulnerabilities leveraged by threat actors in 2018. When exploited, these vulnerabilities allow an unauthenticated attacker to perform remote code executions on Drupal installations, taking full control over the affected website. Following the publication of the proofs of concept in April, thousands of Drupal websites were compromised. This vulnerability has

---

[54] https://blog.trendmicro.com/trendlabs-security-intelligence/malicious-traffic-in-port-7001-surges-as-cryptominers-target-patched-2017-oracle-weblogic-vulnerability/

[55] https://blog.trendmicro.com/trendlabs-security-intelligence/malicious-traffic-in-port-7001-surges-as-cryptominers-target-patched-2017-oracle-weblogic-vulnerability/

[56] https://www.alienvault.com/blogs/labs-research/satan-ransomware-spawns-new-methods-to-spread

[57] https://www.fireeye.com/blog/threat-research/2018/09/click-it-up-targeting-local-government-payment-portals.html

[58] https://threatpost.com/equifax-adds-2-4-million-more-people-to-list-of-those-impacted-by-2017-breach/130209/

[59] https://www.alienvault.com/blogs/labs-research/massminer-malware-targeting-web-servers

[60] https://unit42.paloaltonetworks.com/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall/

[61] https://securityaffairs.co/wordpress/75724/hacking/cve-2018-11776-attacks.html

been leveraged in almost every known attack[62] vector, including deploying various kinds of cryptominers on servers and websites, delivering RATs and Infostealer malware, conducting tech support scams and even establishing massive botnets.[63]

IoT vulnerabilities (CVE-2018-10561, CVE-2018-10562, D-Link Remote Command Execution, MVPower DVR router Remote Code Execution)

The revelation of highly critical flaws in a wide range of router models, and available online proof of concepts, had a significant impact on the IoT threat landscape. These vulnerabilities affected approximately 45% of organizations[64] world-wide. The flaws found in Dasan GPON routers exposed the relevant models to constant attacks, and allowed attackers to obtain sensitive information and gain unauthorized access to the affected device. This year, prominent botnet operators, including Gafgyt,[65] Satori,[66] Mirai[67] and TheMoon,[68] leveraged these flaws to recruit their corps.

According to the Check Point global attack sensors, in 2018, 92% of the attacks observed leveraged vulnerabilities registered in 2017 and earlier. More than 40% of attacks used vulnerabilities that are at least five years old.

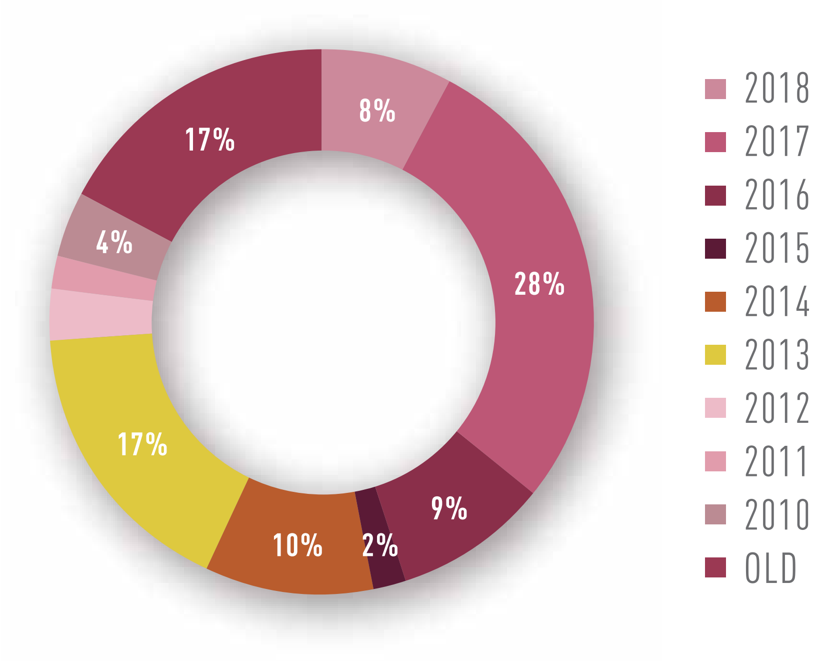


Figure 24: % of attacks that leveraged a new vulnerability discovered in the same year as the observed attack.

---

[62] https://securityaffairs.co/wordpress/72745/cyber-crime/drupal-drupalgeddon-attacks.html

[63] https://www.bleepingcomputer.com/news/security/big-iot-botnet-starts-large-scale-exploitation-of-drupalgeddon-2-vulnerability/

[64] http://blog.checkpoint.com/2018/08/15/julys-most-wanted-malware-attacks-targeting-iot-and-networking-doubled-since-may-2018/

[65] https://researchcenter.paloaltonetworks.com/2018/07/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns/

[66] https://securityaffairs.co/wordpress/72651/hacking/satori-botnet-mass-scanning.html

[67] https://securityaffairs.co/wordpress/72640/malware/wicked-mirai.html

[68] https://securityaffairs.co/wordpress/72762/malware/themoon-gpon-routers.html

APPENDIX C: MALWARE FAMILY DESCRIPTION

MALWARE	DESCRIPTION
Andromeda	Andromeda is a modular bot for malicious activity, and was first spotted in 2011. It is used mainly as a backdoor to deliver additional malware on infected hosts, but can be modified to create different types of botnets.
AdvisorsBot	AdvisorsBot is a sophisticated downloader first spotted in the wild in May 2018. AdvisorsBot has significant anti-analysis features including using "junk code" to slow down reverse engineering, and Windows API function hashing to make it harder to identify the malware's functionality.
Authedmine	Authedmine is a version of the infamous JavaScript miner Coinhive. Like Coinhive, Authedmine is a web-based cryptominer used to perform online mining of Monero cryptocurrency when a user visits a particular web page. Unlike CoinHive, Authedmine requires the website user's explicit consent before running the mining script.
AZORult	AZORult is a Trojan that gathers and exfiltrates data from the infected system. Once the malware is installed on a system (typically delivered by an Exploit Kit such as RIG), it can send saved passwords, local files, crypto-wallets, and computer profile information to a remote C&C server. The Gazorp builder, available on the Dark Web, enables anyone to host an AZORult C&C server with minimal effort.
BadRabbit	BadRabbit is a ransomware that targets the Windows platform. The malware has a list of usernames and passwords to access and spread to SMB shares on other systems in the network. It can also spread via the EternalRomance exploit.
Bancos	Bancos steals financial information, using keylogging to record the victim's credentials as they are entered on a targeted bank webpage. Bancos can also supplement or replace a legitimate bank login page with a fake webpage.
BlackEnergy	BlackEnergy is a Trojan-type program that targets the Windows platform. The malware is designed to delete, block, modify, or copy data and disrupt computer or network performance. The malware masquerades as a legitimate file or software.
Bunitu	Bunitu is a Trojan that targets the Windows platform and sets up a proxy on the infected system to allow malicious activities. Bunitu also adds itself to the list of Windows firewall authorized applications.

MALWARE	DESCRIPTION
Cerber	Cerber, also known as Zerber, was first introduced in February 2016. It is an offline ransomware, meaning that it does not need to communicate with its C2 server before encrypting files on an infected machine.
Chapak	Chapak is a malware dropper and installs malware on the victim's machine after being installed itself. Unlike a downloader, which contacts a remote server to receive access to files, the dropper already contains the malware when installed on the machine. Chapak dropper does not damage the infected computer directly but delivers a malware payload or a number of types of malware with various features.
CNRig	CNRig is a Cryptonight CPU miner for Linux and is based on the open source Monero miner XMRig. CNRig has an automatic update mechanism.
Coinhive	Cryptominer designed to perform online mining of Monero cryptocurrency when a user visits a particular web page. The implanted JavaScript uses a large amount of the end user machines' computational resources, thus impacting their performance.
Cridex	Cridex is a Banking Trojan for the Windows platform. It attempts to steal victim's credentials, such as credit card information. It can download and execute other malicious files on the infected system and is spread via removable drives and network shares.
Cryptoloot	Cryptoloot is a JavaScript cryptominer designed to perform online mining of Monero cryptocurrency when a user visits a particular web page. The implanted JavaScript uses a large amount of the end user machines' computational resources, thus impacting its performance. Cryptoloot is a competitor of Coinhive.
Cryptor	Cryptor is a ransomware which was first discovered in August 2018 and masquerades as the legitimate SuperAntiSpyware Anti-Malware program. Cryptor uses the domain superantispyware.com to distribute the ransomware. Upon encryption, Cryptor creates a ransom note in every folder, which includes a unique victim key and a demand of 0.125 Bitcoin as payment. If the infected machine language and location settings point to Brazil or a Russian-language country, the ransomware does not encrypt the files.
Dorkbot	IRC-based worm that enables remote code execution and downloads additional malware to the infected system. Dorkbot's primary purpose is to steal sensitive information and launch Denial-of-Service attacks.
Dorvku	Dorvku is a Trojan that targets the Windows platform. The malware collects system information and sends it to a remote server. It also collects sensitive information from targeted web browsers.

MALWARE	DESCRIPTION
Emotet	Emotet is an advanced, self-propagating and modular Trojan. Emotet functioned as a banking Trojan, and is currently used to distribute other malware or malicious campaigns. It uses multiple methods for maintaining persistence and evasion techniques to avoid detection. Emotet can also be spread through phishing spam emails.
FileLocker	FileLocker is a ransomware that was first discovered in late 2017, and is a variant of Hidden Tear, the first open-source ransomware for prospectve attackers on GitHub. FileLocker attacks the machines of Korean users. Upon successful infection and encryption, FileLocker demands payment of 50,000 Won (approximately $50) to retrieve the files. Due to a flaw in the malware, a decryptor can be created to retrieve the decryption key from the malware executable.
Fireball	Fireball is an adware distributed by the Chinese digital marketing company Rafotech. It acts as a browser-hijacker which changes the default search engine and installs tracking pixels, and can be turned into a fully functioning malware downloader.
Gafgyt	Gafgyt is a backdoor that targets Linux platforms. This malware spreads as a result of exploiting the vulnerability CVE-2014-6271. Gafgyt contacts a remote server to receive and execute commands on the infected system. These commands include the capability to open a backdoor on the infected system and to perform various DoS attacks.
GandCrab	GandCrab is a ransomware which targets mainly Scandinavia and English-speaking countries. GandCrab is distributed via the RIG and GrandSoft Exploit Kits, as well as email spam. The ransomware is operated in an affiliates program, with those joining the program paying 30%-40% of the ransom revenues to the GandCrab author. In return, affiliates get a full-featured web panel and technical support.
Guerrilla	Guerrilla is an Android Trojan which is embedded in multiple legitimate apps. It downloads additional malicious payloads to generate ad revenue for the app developers.
Hiddad	Hiddad is an Android malware which repackages legitimate apps, and then releases them to a third-party store. Its main function is to display ads. It can also gain access to key security details built into the OS.
HiddenMiner	HiddenMiner is a strain of Android cryptominer that was first seen in April 2018. The HiddenMiner is delivered through a fake Google Play update app, and uses the host device resources to mine Monero.
IcedID	IcedID is a banking Trojan which first appeared in September 2017. It uses other banking Trojans to enable it to spread, including Emotet, Ursnif and Trickbot. IcedID steals user financial data via both redirection attacks (installs local proxy to redirect users to fake web sites) and web injection attacks (injects browser process to present fake content overlaid on top of the original page).

MALWARE	DESCRIPTION
JSEcoin	Web-based cryptominer that performs online mining of Monero cryptocurrency when a user visits a particular web page. The implanted JavaScript uses a large amount of the end user machines' computational resources to mine coins, thus impacting the machine's performance.
Kraken	Kraken is a ransomware Trojan that targets the Windows platform. The malware collects system information and sends it to a remote attacker via the Discord chat service. Kraken downloads and executes the decryptor on the infected system to demand payment for decrypting the files. It can also kill processes on the infected machine.
Lotoor	Lotoor is a hack tool that exploits vulnerabilities on the Android operating system to gain root privileges on compromised mobile devices.
Mirai	Mirai is an Internet-of-Things (IoT) malware that tracks vulnerable IoT devices, such as web cameras, modems and routers, and turns them into bots. Mirai botnet first appeared in September 2016 and quickly made headlines for large-scale attacks, including a massive DDoS attack used to knock the entire country of Liberia offline, and a DDoS attack against the Internet infrastructure firm Dyn, which provides a significant portion of the United States internet's infrastructure.
Necurs	Necurs is one of the largest spam botnets currently active in the wild. In 2016, it was estimated to consist of approximately 6 million bots. The botnet is used to distribute many malware variants, primarily banking Trojans and ransomware.
NetSupportRAT	NetSupportRAT is a commercial Remote Access Tool (RAT) that was developed for system administrators to enable remote access to client machines. However, NetSupport is widely abused by malicious actors to gain unauthorized access to victim machines without their knowledge or consent. The RAT is distributed via fake software updates for Adobe Flash, Google Chrome and Mozilla Firefox. When accessing the compromised website, a malicious JavaScript is downloaded, collects system information and downloads the RAT.
Nivdort	Nivdort is a Trojan family which targets the Windows platform. It gathers passwords and system information or settings such as the Windows version, IP address, software configuration and approximate location.
NotPetya	NotPetya is a ransomware which was spread in a worldwide attack with a high concentration of hits in Ukraine, including the Ukrainian central bank, government offices and private companies. The ransomware has worm capabilities and abuses active sessions and steals credentials. Additionally, NotPetya was used in the "EternalBlue" SMB exploit. After the malware infiltrates into a network, it makes lateral movements to infect the entire network.

MALWARE	DESCRIPTION
OilRig APT	Also known as APT34, OilRig is an Iranian APT group active since 2016, and is believed to be a state-sponsored group under the guidance of the Iranian Intelligence Agency and the Iran Revolutionary Guard Corps (IRGC). The group attacks various targets and organizations across the Middle East, and its primary goal is espionage and sensitive data theft. The victims include mostly financial, aviation, infrastructure, government and university organizations. The group uses spear phishing to deliver its changing payload to its victims.
Olympic Destroyer	Olympic Destroyer is a data wiper malware attributed to the North Korean APT group Lazarus and is spread using the EternalRomance exploit. Olympic Destroyer was utilized in a campaign aimed at the PyeongChang 2018 Winter Olympics, and caused downtime to internal WiFi and television systems, and disrupted some operations during the games' opening ceremony. Olympic Destroyer can hack a computer's data recovery procedures and delete crucial Windows services, causing computers running Windows to be unable to boot.
Panda	Panda is a Zeus variant that was first observed in the wild at the beginning of 2016, and is distributed via Exploit Kits. Since its initial appearance, Panda has targeted financial services in Europe and North America. Before the Olympic Games of 2016, it also ran a special campaign against Brazilian banks.
Parite	Parite is a polymorphic virus which infects executable files on the infected host and on network drive. It drops a malicious DLL file into the Windows temporary directory which is injected into the explorer.exe process.
Pegasus	Pegasus is a highly sophisticated zero-day spyware which targets Android and iOS mobile devices, and is commonly attributed to the Israeli cyber intelligence firm NSO group. Pegasus infects its targets via spear phishing SMS messages which contain a malicious link, and utilizes three zero-day vulnerabilities which allow it to silently jailbreak the device and install the malware. Pegasus features multiple spying modules such as taking screenshots, recording calls, accessing messenger applications, keylogging and exfiltrating browser history. Pegasus is offered for sale, mostly to government-related organizations and corporations.
Qbot	Qbot is a backdoor that drops and downloads other malware. It also establishes a connection with a remote HTTP server without user consent and steals sensitive information.
Ramnit	Ramnit is a banking Trojan which incorporates lateral movement capabilities. Ramnit steals web session information, enabling the worm operators to steal account credentials for all services used by the victim, including bank accounts, corporate and social networks accounts.

MALWARE	DESCRIPTION
RIG Exploit Kit	RIG EK was first introduced in April 2014. It has since received several large updates and continues to be active to this day. RIG is used by many threat actors to distribute malware.
Roaming Mantis	Roaming Mantis is an Android banking Trojan that was first seen in March 2018. It steals users' sensitive information, login credentials and the secret code for two-factor authentication. Roaming Mantis is distributed using DNS hijacking attacks, disguised as Chrome browser or Facebook apps. An evolved version of Roaming Mantis also targets iOS devices with phishing attacks, and desktops and laptops with the Coinhive cryptomining script.
RubyMiner	RubyMiner is a Monero miner that targets both Windows and Linux servers. It seeks out vulnerable versions (such as PHP, Microsoft IIS, and Ruby on Rails) to mobilize them to its mining pool, and to install the open source Monero miner XMRig.
Ryuk	Ryuk is a ransomware used in targeted attacks against several organizations worldwide. The ransomware's technical capabilities are relatively low, and include a basic dropper and a straightforward encryption scheme. Nevertheless, the ransomware caused severe damage and forced victims to pay extremely high ransom payments of up to $320,000 in Bitcoin. Unlike most ransomware, which is distributed via massive spam campaigns and Exploit Kits, Ryuk is used exclusively for targeted attacks. Its encryption scheme is intentionally built for small-scale operations; only crucial assets and resources are infected in each targeted network, and infection and distribution are carried out manually by the attackers.
Sality	Sality is a virus which is spread by infecting .exe and .scr files as well as via removable drives and network shares. Systems infected with Sality can communicate over a peer-to-peer (P2P) network for spamming purposes.
SamSam	SamSam is an independently acting ransomware. After it is installed on a system, it encrypts the files without any need to communicate with a C&C server. SamSam scans for vulnerable servers with unpatched software. Unlike other ransomware campaigns, there is no need for any user action such as clicking a certain link or opening a malicious attachment for the infection to take place. The attackers can trigger the ransomware remotely once it has found vulnerability in the server and penetrated the network. Once a network has been breached, the ransomware spreads through the local network to infect additional computers.
Satan	Satan is a ransomware-as-a-service (RaaS) that was first seen in January 2017. Its developers offer a user-friendly web portal with customization options, allowing anyone who buys it to create custom versions of Satan ransomware and distribute it to victims. New versions of Satan were observed using the EternalBlue exploit to spread across compromised environments, as well as performing lateral movement using other exploits.

MALWARE	DESCRIPTION
Satori	Satori is a variant of the Mirai IoT botnet. The payload delivered by an IoT (Internet of Things) botnet targets vulnerable HG532 Huawei home routers, and is based on a zero-day vulnerability in the device. After infection, the botnet utilizes the infected machines for various purposes including cryptocurrency mining and credentials theft. The attack was first identified by Check Point researchers in November 2017.
Scarsi	Scarsi is a malware used to infect as many victims as possible to form a botnet, a network of computers, usually controlled by the owner via C&C servers, for illicit purposes such as DDoS attacks, mining cryptocurrency, mail spam, etc.
Stone Panda APT	Also known by the nickname APT10, Stone Panda is an elite APT group active since 2009, and is believed to be of Chinese origin and state sponsorship. The group's primary goal is intellectual property theft and it often targets government documents of national security importance. Stone Panda's most notable attack included a well-planned operation which targeted MSSP providers worldwide which were leveraged by the group to gain access to the networks of several of their customers. Its targets are spread worldwide, but APT10 heavily attacks US-based and Japanese companies belonging to both the business and government sectors.
TheMoon	TheMoon is a botnet which appeared in 2014 and infected Linux servers. In 2017, it switched to IoT devices. In 2018, the botnet integrated a new zero-day exploit for the Dasan GPON router into its code, allowing its operators to recruit them to the botnet.
TheTruthSpy	TheTruthSpy is an Android spyware first seen in May 2017. It monitors WhatsApp messages, Facebook chats, and internet browsing history.
Tinba	Tinba is a banking Trojan which targets mainly European banking customers and uses the Blackhole Exploit Kit. Tinba steals the victim's credentials using web-injects, which are activated as the user tries to connect his account.
Triada	Triada is a modular backdoor for Android which grants super-user privileges to download second stage malware. Triada has also been seen spoofing URLs loaded in the browser.
Trickbot	Trickbot is a Dyre variant that appeared in October 2016. Since its first appearance, it has targeted primarily banks in Australia and the UK, and lately also in India, Singapore and Malesia.
Virut	Virut is a major botnet and malware distributor in the Internet, and is used in DDoS attacks, spam distribution, data theft and fraud. The malware is spread through executables originating from infected devices such as USB sticks as well as compromised websites, and attempts to infect any executable file. Virut alters the local host files and opens a backdoor by joining an IRC channel controlled by a remote attacker.

MALWARE	DESCRIPTION
VPNFilter	VPNFilter is a Trojan that targets Linux operating systems running on MIPS and x86 architectures. The malware downloads a binary from a control server and executes it. The downloaded binary retrieves and executes commands from the control server which allows it to execute shell commands, disable the device, upload files, and more. It has been reported that this malware is capable of modifying NVRAM values. Furthermore, this malware may achieve persistence by adding itself to the Chrome tab.
WannaCry	WannaCry is a ransomware which was spread in a large scale attack in May 2017, and utilizes a Windows SMB exploit called EternalBlue to propagate within and between networks.
WannaMine	WannaMine is a sophisticated Monero cryptomining worm that spreads utilizing the EternalBlue exploit. WannaMine implements a spreading mechanism and persistence techniques by leveraging Windows Management Instrumentation (WMI) permanent event subscriptions.
XMRig	XMRig is open-source CPU mining software used for mining Monero cryptocurrency. It was first seen in the wild in May 2017.
Zacinlo	Zacinlo is a highly sophisticated and persistent malware that targets the Window platform and has been active since 2012. Zacinlo takes screenshots, spams the system with advertisements, opens multiple browser sessions and replaces legitimate ads on a website with its own ads, and designs specially crafted ads to manipulate users into clicking them. Zacinlo can also carry out man-in-the-middle (MitM) attacks to intercept traffic, detect and remove competing adware and also any local services it deems dangerous such as security software.
Zapchast	Zapchast is an IRC-controlled backdoor that allows an attacker to access and control an affected machine. When the backdoor is run, it establishes a connection to an IRC (Internet Relay Chat) server. It then creates a bot in a specific IRC channel or server, and uses the channel to control its multiple bots and launch distributed denial of service (DDoS) attacks.
Zeus	Zeus is a widely distributed Windows Trojan which is mostly used to steal banking information. When a machine is compromised, the malware sends information such as the account credentials to the attackers using a chain of C&C servers.

Check Point®
SOFTWARE TECHNOLOGIES LTD

cp<r>
CHECK POINT RESEARCH

WORLDWIDE HEADQUARTERS

5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-1100
Email: info@checkpoint.com

U.S. HEADQUARTERS

959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-4391 | 650-628-2000 | Fax: 650-654-4233

UNDER ATTACK?

Contact our Incident Response Team:
emergency-response@checkpoint.com

checkpoint.com